

日 本 国 特 許 庁

JAPAN PATENT OFFICE

07.01.03

REC'D 03 MAR 2003

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 1月 8日

出 願 番 号

Application Number:

特願2002-001843

[ST.10/C]:

[JP2002-001843]

出 願 人

Applicant(s):

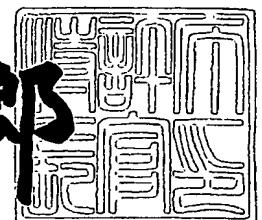
株式会社エヌ・ティ・ティ・ドコモ

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2003年 2月12日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3006544

【書類名】 特許願

【整理番号】 DCMH130548

【提出日】 平成14年 1月 8日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/00

【発明の名称】 配信方法および配信システム

【請求項の数】 19

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ ティ・ ドコモ内

【氏名】 山田 和宏

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ ティ・ ドコモ内

【氏名】 渡邊 信之

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ ティ・ ドコモ内

【氏名】 津田 雅之

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ ティ・ ドコモ内

【氏名】 神谷 大

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ ティ・ ドコモ内

【氏名】 浅井 真生

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ

・ ティ・ ティ・ ドコモ内

【氏名】 三浦 史光

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ ティ・ ドコモ内

【氏名】 鷺尾 諭

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ ティ・ ドコモ内

【氏名】 富岡 淳樹

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ ティ・ ドコモ内

【氏名】 川端 博史

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
・ ティ・ ティ・ ドコモ内

【氏名】 近藤 隆

【特許出願人】

【識別番号】 392026693

【氏名又は名称】 株式会社エヌ・ ティ・ ティ・ ドコモ

【代理人】

【識別番号】 100098084

【弁理士】

【氏名又は名称】 川▲崎▼ 研二

【選任した代理人】

【識別番号】 100111763

【弁理士】

【氏名又は名称】 松本 隆

【手数料の表示】

【予納台帳番号】 038265

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 配信方法および配信システム

【特許請求の範囲】

【請求項 1】 アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置を示すアプリケーション記述ファイルを格納した情報提供サーバ装置と、前記アプリケーション記述ファイルの格納位置を示す第 1 の識別情報と前記端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報とを内包したセキュリティ記述ファイルを格納した管理サーバ装置とを有し、ファイルの格納位置を通知されると当該ファイルを返送する通信システムが、アプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置へ前記セキュリティ記述ファイルを、セキュリティを確保して送信する権限送信過程と、

前記端末装置が、前記権限送信過程にて前記通信システムから送信された前記セキュリティ記述ファイルに内包されている前記第 1 の識別情報を用いて前記アプリケーション記述ファイルを取得する依存情報取得過程と、

前記端末装置が、前記依存情報取得過程にて取得した前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得するプログラム取得過程と

を有する配信方法。

【請求項 2】 前記通信システムはセキュリティの確保された通信路を介して前記セキュリティ記述ファイルを送信することによりセキュリティを確保する請求項 1 に記載の配信方法。

【請求項 3】 前記通信路は暗号化されている請求項 2 に記載の配信方法。

【請求項 4】 前記通信路は移動通信網および専用線により実現される請求項 2 に記載の配信方法。

【請求項 5】 前記通信路は移動通信網および暗号化された通信路により実

現される

請求項 2 に記載の配信方法。

【請求項 6】 前記通信システムが前記セキュリティ記述ファイルを暗号化する暗号化過程と、

前記端末装置が、前記権限送信過程にて前記通信システムから送信された前記セキュリティ記述ファイルを復号する復号過程とを有し、

前記権限送信過程では、前記暗号化過程にて暗号化された前記セキュリティ記述ファイルを前記端末装置へ送信し、

前記依存情報取得過程では、前記端末装置が、前記復号過程にて復号された前記セキュリティ記述ファイルを用いて前記アプリケーション記述ファイルを取得する

請求項 1 に記載の配信方法。

【請求項 7】 前記権限情報は資源の利用に関する制限を示す

請求項 1 に記載の配信方法。

【請求項 8】 前記資源は前記端末装置内部のハードウェア資源である

請求項 7 に記載の配信方法。

【請求項 9】 前記資源は前記端末装置外部の、前記端末装置が使用可能なハードウェア資源である

請求項 7 に記載の配信方法。

【請求項 10】 前記資源は前記端末装置内部のソフトウェア資源である

請求項 7 に記載の配信方法。

【請求項 11】 前記資源は前記端末装置外部の、前記端末装置が使用可能なソフトウェア資源である

請求項 7 に記載の配信方法。

【請求項 12】 前記資源は、前記端末装置が使用可能なネットワーク資源である

請求項 7 に記載の配信方法。

【請求項 13】 前記権限情報は資源の利用の種類を示す

請求項 1 に記載の配信方法。

【請求項14】 前記アプリケーションに対応するアプリケーション記述ファイルは前記アプリケーションを提供する情報提供事業者に対して認証局が与えた秘密鍵で署名されており、かつ、前記アプリケーションに対応するセキュリティ記述ファイルは前記情報提供事業者に対して認証局が与えた公開鍵を内包し、

前記プログラム取得過程では、前記端末装置が、前記依存情報取得過程で取得したアプリケーション記述ファイルの正当性を前記公開鍵を用いて検証し、正当性が検証された場合にのみ、当該アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する

請求項1に記載の配信方法。

【請求項15】 前記アプリケーション記述ファイルおよび前記セキュリティ記述ファイルは、前記管理サーバ装置を管理する管理者が付与するアプリケーション識別子を内包し、

前記プログラム取得過程では、前記端末装置が、前記権限送信過程で前記管理サーバ装置から送信されたセキュリティ記述ファイルに内包されたアプリケーション識別子と前記依存情報取得過程で取得したアプリケーション記述ファイルに内包されたアプリケーション識別子とを比較し、両者が一致した場合にのみ、当該アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する

請求項1に記載の配信方法。

【請求項16】 前記通信システムは、さらに、前記セキュリティ記述ファイルの格納位置を示す第2の識別情報を内包したダウンロード用ファイルを格納した情報提供サーバ装置を有し、

前記通信システムが端末装置へ前記ダウンロード用ファイルを送信する事前送信過程と、

前記端末装置が、前記事前送信過程にて前記通信システムから送信された前記ダウンロード用ファイルを用いて前記セキュリティ記述ファイルの送信を前記通信システムに要求する権限送信要求過程とを有し、

前記権限送信過程では、前記通信システムが、前記権限送信要求過程にて要求された前記セキュリティ記述ファイルを前記端末装置へ送信する

請求項 1 に記載の配信方法。

【請求項 17】 前記依存情報送信過程にて送信されるセキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ前記依存情報取得過程以降の過程を実行する

請求項 1 に記載の配信方法。

【請求項 18】 前記端末装置は移動機である

請求項 1 ～請求項 17 のいずれかの請求項に記載の配信方法。

【請求項 19】 アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置を示すアプリケーション記述ファイルを格納した情報提供サーバ装置と、前記アプリケーション記述ファイルの格納位置を示す第 1 の識別情報と前記端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報とを内包したセキュリティ記述ファイルを格納した管理サーバ装置とを有し、ファイルの格納位置を通知されると当該ファイルを返送する通信システムと、

アプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置とを有し、

前記管理サーバ装置は、前記セキュリティ記述ファイルを前記端末装置へ、セキュリティを確保して送信し、

前記端末装置は、前記通信システムから送信された前記セキュリティ記述ファイルに内包されている前記第 1 の識別情報を用いて前記アプリケーション記述ファイルを取得し、前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する

配信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、端末装置にアプリケーションを配信する技術に関する。

【0002】

【従来の技術】

J a v a（登録商標）プログラミング言語に従って記述されたプログラムを実行してJ a v a - A P（J a v aアプリケーション）を実現する機能を備え、この種のプログラムを含むソフトウェアであるJ a v a - A Pソフトウェアを、ネットワークを介してダウンロードすることができる移動機が普及している。この種の移動機によるJ a v a - A Pソフトウェアのダウンロード手順は、WWW（World Wide Web）を構成するサーバ装置からA D F（Application Descriptor File）を取得し、次いでJ a r（Java Archive）ファイルを取得するという流れになっている。

【0003】

A D FはJ a rファイルに依存した内容となっており、例えば、J a rファイルの格納位置を示すU R L（以後、パッケージU R L）、J a rファイルのサイズを示す情報、J a rファイルの最終変更日時を示す情報等を必須情報として内包している。A D Fを取得した移動機はこのA D Fの内容を調べ、ダウンロードしようとしているJ a v a - A Pソフトウェアを当該移動機にインストール可能であるか否かを判断する。

【0004】

インストール可能と判断すると、移動機は、WWWを構成するサーバ装置からパッケージU R Lを用いてJ a rファイルを取得する。J a rファイルには、J a v a - A Pソフトウェアが格納されており、J a rファイルの取得をもってJ a v a - A Pソフトウェアのダウンロードは完了する。以後、移動機において、当該J a v a - A Pソフトウェアが起動可能に設定され、当該J a v a - A Pソフトウェアのインストールが完了する。

【0005】

【発明が解決しようとする課題】

ところで、移動機内に実現されるJ a v a - A Pの挙動についての制限は、通信アプリケーションなどの移動機が元から備えているネイティブアプリケーションの挙動についての制限よりも厳しくなっている。例えば、J a v a - A Pは、移動機内の電話帳データを参照することができないようになっている。このよう

な制限の相違により、悪意をもって作成された J a v a - A P、あるいは不具合を有する J a v a - A P によって移動機内の秘密性の高い情報が漏洩したり改竄されたりする事態を確実に回避することができる。

【0006】

しかし、上述した厳しい制限を全ての J a v a - A P に対して一律に課すだけでは、ユーザや I P（情報提供事業者）の希望を満たすことはできない。例えば、ある程度の信頼性が保証されるのであれば、J a v a - A P に移動機に格納された個人情報を参照する権限を与えてもよいと感じるユーザが少なくないと思われる。また、I P にも、移動機に格納されている個人情報や移動機が有する多数の機能の使用を前提とした J a v a - A P を提供したいという希望がある。

【0007】

これらの希望を満たす仕組みとして、移動機のユーザに対して通信サービスを提供する通信事業者等の信頼できる機関が J a v a - A P に権限を与え、この権限を移動機に通知し、当該権限に基づいて移動機が当該 J a v a - A P の挙動を制限するという仕組みが考えられる。この仕組みでは、権限の信頼性を保証するために、信頼できる機関以外の他者が権限の付与・管理に関与し得ないようにすべきである。

【0008】

J a v a - A P ソフトウェアのダウンロード手順に上述の仕組みを適用する場合、A D F あるいは J a r ファイルに権限を示す情報を内包させるのが妥当である。J a r ファイルは I P により随時更新される種類のファイルであり、I P が保有するのが妥当であることから、信頼できる機関に保有させるなら A D F が妥当ということになる。

【0009】

しかし、A D F は J a r ファイルに依存した内容となることから、I P が手元の J a r ファイルを更新されると、信頼できる機関が保有している A D F の更新も必要になってくる。A D F は信頼できる機関において他者の他の関与を排するように管理されるのであるから、A D F の更新作業は繁雑な作業となると予想される。また、J a r ファイルを更新せずとも、A D F の更新が必要となることが

ある。例えば、IPにおいて、あるJarファイルへのアクセスが集中し、このJarファイルを他のサーバ装置へ移動する場合である。この場合、Jarファイルの格納位置が変更されるから、ADFに内包されているパッケージURLを変更する必要がある。

【0010】

本発明は、上述した事情に鑑みて為されたものであり、依存関係にある複数のファイルを配信することで配信される、アプリケーションを実現するためのソフトウェアを、IPの自由度を制限することなく、権限に応じた挙動をアプリケーションに対して許可する端末装置へ配信する配信方法および配信システムを提供することを目的としている。

【0011】

【課題を解決するための手段】

上述した課題を解決するために、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置を示すアプリケーション記述ファイルを格納した情報提供サーバ装置と、前記アプリケーション記述ファイルの格納位置を示す第1の識別情報と前記端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報とを内包したセキュリティ記述ファイルを格納した管理サーバ装置とを有し、ファイルの格納位置を通知されると当該ファイルを返送する通信システムが、アプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置へ前記セキュリティ記述ファイルを、セキュリティを確保して送信する権限送信過程と、前記端末装置が、前記権限送信過程にて前記管理サーバ装置から送信された前記セキュリティ記述ファイルに内包されている前記第1の識別情報を用いて前記アプリケーション記述ファイルを取得する依存情報取得過程と、前記端末装置が、前記依存情報取得過程にて取得した前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得するプログラム取得過程とを有する配信方法を提供する。

【0012】

この配信方法によれば、端末装置は、アプリケーションに対応したアプリケーション記述ファイルおよび実体ファイルを取得する前に、セキュリティが確保された上で通信システムから送信されるセキュリティ記述ファイルを取得する。このセキュリティ記述ファイルにはアプリケーションに与えられた権限が示されており、端末装置では、取得したセキュリティ記述ファイルに示される権限に応じた挙動が当該セキュリティ記述ファイルに対応するアプリケーションに許可される。

【0013】

また、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置を示すアプリケーション記述ファイルを格納した情報提供サーバ装置と、前記アプリケーション記述ファイルの格納位置を示す第1の識別情報と前記端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報とを内包したセキュリティ記述ファイルを格納した管理サーバ装置とを有し、ファイルの格納位置を通知されると当該ファイルを返送する通信システムと、

アプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置とを有し、

前記管理サーバ装置は、前記セキュリティ記述ファイルを前記端末装置へ、セキュリティを確保して送信し、前記端末装置は、前記通信システムから送信された前記セキュリティ記述ファイルに内包されている前記第1の識別情報を用いて前記アプリケーション記述ファイルを取得し、前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する配信システムを提供する。

【0014】

この配信システムによれば、端末装置は、アプリケーションに対応したアプリケーション記述ファイルおよび実体ファイルを取得する前に、セキュリティが確保された上で通信システムから送信されるセキュリティ記述ファイルを取得することになる。このセキュリティ記述ファイルにはアプリケーションに与えられた

権限が示されており、端末装置では、取得したセキュリティ記述ファイルに示される権限に応じた挙動が当該セキュリティ記述ファイルに対応するアプリケーションに許可される。

【0015】

【発明の実施の形態】

以下、図面を参照して、本発明の実施の一形態である配信システムについて図面を参照して説明する。なお、図面において、共通する部分には同一の符号が付されている。

この配信システムは、移動通信網を管理する通信事業者（信頼できる機関）が、移動機にインストール可能なJava-APソフトウェアをダウンロードするための情報を移動機のユーザへ提示し、この提示を受けたユーザが、移動機を操作して所望のJava-APソフトウェアを移動機にダウンロードおよびインストールし、移動機において起動するためのものである。なお、本システムにおけるJava-APソフトウェアのダウンロードは、当該Java-APソフトウェアの内容を説明した画面を移動機のユーザに提示した後にADFを配信し更にJarファイルを配信するという手順で行われる。

【0016】

（1）構成

図1に示されるように、この配信システムは、インターネット11に接続されたIPサーバ装置12～14と、通信事業者が移動パケット通信サービスを提供するために用いる移動パケット通信網15との間で無線パケット通信を行うことが可能であり、移動パケット通信網15を介して通信相手とパケット通信を行うことができる移動機16と、インターネット11と移動パケット通信網15とを相互接続するゲートウェイサーバ装置17と、専用線によりゲートウェイサーバ装置17に接続された管理サーバ装置18とを有する。このシステムには多数の移動機が存在するが、図面が繁雑になるのを避けるために一つの移動機16のみが図示されている。これと同様の理由により、3つのIPサーバ装置12～14のみが図示されている。

【0017】

(1-1) IPサーバ装置

IPサーバ装置12は第1のIPに管理されており、IPサーバ装置13および14は第1のIPと異なる第2のIPにより管理されている。IPサーバ装置12～14はWWWを構成しており、それぞれ一般的なWWWサーバ装置と同様のハードウェアおよび機能を有する。また、IPサーバ装置12は不揮発性メモリ12A、IPサーバ装置13は不揮発性メモリ13A、IPサーバ装置14は不揮発性メモリ14Aを有し、IPサーバ装置12～14はそれぞれ、TCPに従ったコネクション（以後、TCPコネクション）を通信相手との間に確立し、このコネクションを介してHTTPのGETメソッドを用いた要求メッセージを受信すると、当該GETメソッドに指定されたURLで特定されるファイルを自身の不揮発性メモリから読み出し、このファイルを含むHTTPの応答メッセージを返送して当該コネクションを切断する。

【0018】

不揮発性メモリ12A、13Aおよび14Aはそれぞれハードディスク等の不揮発性メモリであり、Javaプログラミング言語を用いて作成されたプログラムを有するJarファイルと、当該Jarファイルに関する情報を記述したADFと、当該プログラムを内包するJava-APソフトウェアの内容を移動機のユーザに説明するための説明ファイルとを記憶し得る。

【0019】

IPサーバ装置に格納され得るADFには後述するトラステッドJava-APソフトウェアに対応したADFと、非トラステッドJava-APソフトウェアに対応したADFとがある。WWWにおけるJarファイルの記憶位置を示すパッケージURLや、Jarファイルのサイズを示す情報、Jarファイルの最終変更日時を示す情報等の従来からADFに記述されている情報は両者にも記述される。これに加えて、トラステッドJava-APソフトウェアに対応したADFは、図2に示されるように、後述するAPIDとJarファイルのハッシュ値とを内包し、さらに当該ソフトウェアを提供するIPに対してCA（認証局）から付与された秘密鍵で署名される。

【0020】

また、説明ファイルはHTMLに従って記述されるテキストファイルであり、移動機においてHTMLに従って解釈されたときに、このファイルに対応するJava-APソフトウェアをダウンロードするときにユーザにより操作されるオブジェクトと当該Java-APソフトウェアに対応するSDF（セキュリティ記述ファイル。SDFが存在しない場合にはADF）がWWWにおいて記憶されている位置を示すURLとが対応付けられたUI（ユーザインターフェイス）が提供されるように記述されている。なお、SDFについては後述する。

また、IPサーバ装置12～14の各々は、対応するIPの指示に従って上記各ファイルを作成および更新する機能を備えている。

【0021】

（1-2）ゲートウェイサーバ装置

ゲートウェイサーバ装置17は前述の通信事業者により管理されており、移動パケット通信網15とインターネット11とを接続する一般的なゲートウェイサーバ装置と同様の構成を有し、移動パケット通信網15とインターネット11と管理サーバ装置18との間で相互に通信を中継する。

【0022】

（1-3）管理サーバ装置

管理サーバ装置18は前述の通信事業者により管理されており、WWWを構成し、一般的なWWWサーバ装置と同様のハードウェアおよび機能を有する。また、管理サーバ装置18はハードディスク等の不揮発性メモリ18Aを有し、TCPコネクションを通信相手との間に確立し、このコネクションを介してHTTPのGETメソッドを用いた要求メッセージを受信すると、当該GETメソッドに指定されたURLで特定されるファイルを不揮発性メモリ18Aから読み出し、このファイルを含むHTTPの応答メッセージを返送して当該コネクションを切断する。

【0023】

また、上記不揮発性メモリ18Aには、移動機16にダウンロード可能なJava-APソフトウェアを移動機16のユーザに紹介するためのリストファイル200と、移動機のトラステッドAPI（Application Interface）を使用する

J a v a - A P を移動機において実現するための J a v a - A P ソフトウェアを移動機にダウンロードする際に必須のファイルであって、当該 J a v a - A P ソフトウェアについて上記通信事業者と当該 J a v a - A P ソフトウェアを提供する I P との間で結ばれた契約に従って当該通信事業者により作成される S D F とが記憶される。なお、トラステッド A P I については後述する。

【0024】

上記リストファイル 200 は HTML に従って記述されたテキストファイルであり、HTML に従って解釈された場合に、J a v a - A P ソフトウェア毎に対応した選択肢と、当該 J a v a - A P ソフトウェアの説明ファイルが WWW において記憶されている位置を示す URL とが対応付けられた U I が提供されるように記述されている。

【0025】

(1-4) 移動機

移動機 16 は、図 3 に示されるように、移動機 16 は、OS (オペレーティングシステム) ソフトウェア、J a v a - A P を実行する環境を構築するための J a v a - A P 環境ソフトウェア、および各種ネイティブ A P ソフトウェア等を記憶した ROM 16 A と、ROM 16 A に接続され ROM 16 A からプログラムを読み出して実行する CPU 16 B と、CPU 16 B に接続された表示部 16 C、不揮発性メモリ 16 D、RAM 16 E、通信部 16 F および操作部 16 G を有する。

【0026】

表示部 16 C は例えば液晶表示パネルを有し、CPU 16 B から供給されるデータで表される画像を表示する。不揮発性メモリ 16 D は例えば S R A M や E E P R O M であり、CPU 16 B によりデータを読み書きされる。詳しくは後述するが、不揮発性メモリ 16 D は、WWW を構成するサーバ装置 (以後、W e b サーバ装置) からダウンロードした J a v a - A P ソフトウェア (A D F および J a r を内包する) や、S D F を記憶するために使用される。

【0027】

通信部 16 F は移動パケット通信網 15 と無線パケット通信を行うものであり

、CPU16Bと移動パケット通信網15との間でパケットを中継する。また、通信部16Fは、アンテナや無線送受信部の他に、通話のためのCODECやマイク、スピーカ等を備えており、移動機16は図示せぬ移動通信網を介して回線交換による通話を行うこともできる。操作部16Gは操作子を備え、操作子の操作に応じた信号をCPU16Bへ供給する。

【0028】

図示せぬ電源が投入されると、CPU16BはRAM16Eをワークエリアとし、ROM16AからOSソフトウェアに内包されているプログラムを読み出して実行する。これにより、CPU16BにはUI等を提供する機能が実現される。すなわち、CPU16BはOSソフトウェアを起動して移動機16内にて図4のOSを実現する。OSは操作部16Gから供給される信号とUIの状態とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。

【0029】

ユーザの指示がネイティブAPソフトウェアである通信ソフトウェアの起動を要求するものであれば、OSは通信ソフトウェアを起動して移動機16内にて通信APを実現する。この通信APを用いることで、ユーザは通話相手と通話を行うことができる。

【0030】

ユーザの指示がネイティブAPソフトウェアである電話帳APの起動を要求するものであれば、OSは電話帳ソフトウェアを起動して移動機16内にて電話帳APを実現する。この電話帳APを用いることで、ユーザは、不揮発性メモリ16Dに記憶された電話帳の内容（以後、電話帳データ）を参照・使用・変更することができる。

【0031】

ユーザの指示がネイティブAPソフトウェアであるWebブラウザソフトウェアの起動を要求するものであれば、OSはWebブラウザソフトウェアを起動して移動機16内にてWebブラウザを実現する。WebブラウザはUIを提供し、このUIの状態と操作部16Gから供給される信号とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。例えば、当該指示が指定されたファイ

ルをWWWから取得する旨の指示の場合には、通信部16Fを制御して当該ファイルを記憶したWebサーバ装置との間にTCPコネクションを確立し、このコネクションを介して、指定された位置を示すURLをGETメソッドに指定したHTTPの要求メッセージを送信し、この要求メッセージに対応する応答メッセージを受信し、当該コネクションを切断する。さらに、Webブラウザは、受信した応答メッセージに内包されているファイルをHTMLに従って解釈し、Webページを内包するUIを生成し、ユーザに提供する。また、ユーザの指示がJava-APソフトウェアのダウンロードを要求するものである場合には、この指示を次に述べるJAM (Java Application Manager) に通知する。具体的には、Webページにおいて、オブジェクトタグが指定されているアンカータグで表されるアンカーが押下（クリック操作またはプレス操作）されると、Webブラウザは当該オブジェクトタグのdata属性に指定されているURLを抽出し、当該URLからのJava-APソフトウェアのダウンロードが要求されたことをJAMに通知する。

【0032】

ユーザの指示がネイティブAPソフトウェアであるJAMソフトウェアの起動を要求するものであれば、OSはJAMソフトウェアを起動して移動機16内にJAMを実現する。JAMは、移動機16にインストールされているJava-APソフトウェアの一覧をユーザに提示し、ユーザにより指定されたJava-APソフトウェアを起動する。具体的には、JAMに対するユーザの指示がJava-APソフトウェアの起動を要求するものであれば、Java-AP環境ソフトウェアが起動されて移動機16内にJava-AP環境が実現され、次に、指定されたJava-APソフトウェアが起動されてJava-AP環境内にJava-APが実現される。Java-AP環境は、携帯端末に適した軽量のJava仮想マシンであるKVMと、Java-APに対して提供されるAPIとを有する。Java-APに対して提供されるAPIは、通信事業者がIPとの契約に基づいて信頼性を保証したJava-AP（以後、トラステッドAP）のみに使用が許可されるトラステッドAPIと、あらゆるJava-APに使用が許可される非トラステッドAPIとに分けられる。

【0033】

また、JAMは、Java-APのダウンロードを要求する指示がWebブラウザから通知されると、Java-APソフトウェアを移動機16にダウンロードしインストールする処理を行う。この処理の流れを図5に示す。

図5に示されるように、JAMは、まず、ダウンロードしようとするJava-APソフトウェアがトラステッドAPを実現するためのJava-APソフトウェア（以後、トラステッドJava-APソフトウェア）であるか否かを判定する（ステップS11）。具体的には、JAMは、Webブラウザから通知されたURLの末尾のファイル名を参照し、このファイルの拡張子が“sdf”であればトラステッドJava-APソフトウェア、“sdf”でなければ非トラステッドJava-APソフトウェアであると判定する。ダウンロードしようとするJava-APソフトウェアがトラステッドJava-APソフトウェアであると判定された場合には、従来と同様のダウンロードおよびインストール処理が行われる（ステップS12）。

【0034】

ダウンロードしようとするJava-APソフトウェアがトラステッドJava-APソフトウェアと判定された場合には、JAMは、当該ソフトウェアに対応するSDFを管理サーバ装置18から取得する（ステップS13）。すなわち、JAMは、管理サーバ装置18との間にTCPコネクションを確立し、このコネクションを介して、Webブラウザから通知されたURLで示される位置に記憶されたSDFの送信を管理サーバ装置18に要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し、上記コネクションを切断する。

【0035】

SDFは、トラステッドAP毎に通信事業者により作成されるファイルであり、図6に示されるように、トラステッドJava-APソフトウェアを一意に識別するためのAPID、後述するポリシー情報、当該Java-APソフトウェアに対応したADFの記憶位置を示すURLであるADF-URL、および当該Java-APソフトウェアを提供するIPに対してCAが付与した公開鍵を有

する。JAMは、応答メッセージに内包されているSDFからAPIDとADF-URLと公開鍵を抽出するとともに、当該SDFを不揮発性メモリ16Dに書き込む。

【0036】

次に、JAMはADFを取得する（ステップS14）。具体的には、JAMは、SDFから抽出したADF-URLで特定されるADFを記憶したWebサーバ装置との間にTCPコネクションを確立し、当該ADFの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し、当該TCPコネクションを切断する。

【0037】

トラステッドJava-APソフトウェアに対応するADFは非トラステッドJava-APソフトウェアに対応する通常のADFとは異なり、前述のAPIDとJarファイルのハッシュ値とを内包し、さらに当該トラステッドJava-APソフトウェアを提供するIPに対してCAが付与した秘密鍵により署名（暗号化）されている。JAMは、応答メッセージに内包されているADFの署名をSDFから抽出された公開鍵を用いて検証し（復号し）、当該ADFの正当性を判断する（ステップS15）。

【0038】

ADFが正当であると判断した場合には、JAMは、SDFから抽出したAPIDとADFに内包されているAPIDとを比較し、両者が一致するか否かを判定する（ステップS16）。両者が一致すると判定された場合には、JAMは、当該トラステッドJava-APソフトウェアを移動機16にインストール可能か否かをADFの内容に基づいて判定する（ステップS17）。この判定の基準は従来と同様である。

【0039】

インストール可能と判定された場合には、JAMは、Jarファイルを取得する。具体的には、JAMは、当該ADFを移動機16に書き込むとともに、当該ADFからハッシュ値とパッケージURLを抽出する。さらにJAMは、このパッケージURLで特定されるJarファイルを記憶したWebサーバ装置との間

にTCPコネクションを確立し、当該Jarファイルの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し、当該TCPコネクションを切断する（ステップS18）。

【0040】

さらに、JAMは、取得したJarファイルに対するハッシュ値を算出する（ステップS19）。ハッシュ値の算出に使用するハッシュ関数は任意であるが、移動機で使用されるハッシュ関数とADFに含まれるハッシュ値の算出時に使用されるハッシュ関数は一致していなければならない。実際には、移動機で 사용되는ハッシュ関数を用いて、トラステッドJava-APソフトウェアを提供するIPがハッシュ値を算出してADFを生成することになる。

【0041】

JAMは、JAMが算出したハッシュ値とADFから抽出したハッシュ値とを比較し（ステップS20）、両者が一致した場合には、取得したJarファイルを管理サーバ装置18に書き込み、トラステッドJava-APソフトウェアのインストールに係る各種処理を行い（ステップS21）、インストールに成功した旨をユーザに通知する（ステップS22）。

【0042】

なお、ADFが正当でないと判断した場合、SDFが有するAPIDとADFが有するAPIDが不一致の場合、インストールしようとするJava-APソフトウェアをインストール可能ではないと判断した場合、算出したハッシュ値とADFが有するハッシュ値とが不一致の場合には、JAMは、インストールに失敗した旨をユーザに通知するとともに、移動機16の状態を、SDFの取得を開始する前の状態に戻す。

【0043】

また、JAMは、Java-APの挙動を監視し、トラステッドAPIの使用を制限する。この制限は不揮発性メモリ16Dに記憶されるSDF内のポリシー情報に従って行われる。SDF内のポリシー情報は、例えば図7に概念的に示されるような内容となっている。図7に示されるポリシー情報では、移動機に格納された電話帳データを参照するときに必須のトラステッドAPIである“getPho

neList()”と移動機の状態を取得するときに必須のトラステッドAPIである“getMsStatus()”の使用が許可され、移動機に格納された発着信履歴データを参照するときに必須のトラステッドAPIである“getCallHistory()”の使用が禁止されている。

【0044】

(2) 動作例

次に、上述したシステムの動作例について説明する。

なお、以下に述べる動作において、TCPコネクションの確立および切断動作についてはHTTPにおける一般的な動作となることから、それらの説明を省略する。また、前述のOS、Webブラウザ、JAM、Java-Ap、ネイティブAp等が行う動作は移動機16の動作となることから、以降の説明では、動作の主体を移動機16とする。

また、図8に示されるように、管理サーバ装置18の不揮発性メモリ18Aには、リストファイル200とSDF204が記憶されているものとする。これらはIPサーバ装置13およびIPサーバ装置14を管理するIPと管理サーバ装置18を管理する通信事業者との間で結ばれた契約に従って通信事業者により作成されている。これらのうち、リストファイル200は、移動機16において解釈・実行されると図9に示されるリストページ201を提供するように記述されている。また、リストファイル200は、リストページ201を構成する選択肢201Aが押下されると（クリックまたはプレスされると）、後述の説明ファイル202のURL（“http://www.main.bbb.co.jp/ghi.html”）をGETメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。さらに、リストファイル200は、リストページ201を構成する選択肢201Bが押下されると（クリックまたはプレスされると）、後述の説明ファイル207のURL（“http://www.ccc.co.jp/jkl.html”）をGETメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。

【0045】

また、SDF204は、APIDとして“0001”、ポリシー情報として図7に示される内容の情報、ADF-URLとして“http://www.main.bbb.co.jp/view

er.jam”、および公開鍵としてIPサーバ装置13およびIPサーバ装置14を管理するIPに対してCAが付与した公開鍵を内包している。

【0046】

また、IPサーバ装置12の不揮発性メモリ12Aには、「詰め将棋」なる名称のJava-APソフトウェア（以後、第1のJava-APソフトウェア）に対応する説明ファイル211、ADF213およびJarファイル214が記憶されているものとする。これらはIPサーバ装置12を管理するIPによって作成されている。これらのうち、説明ファイル211の内容は図10に示される通りであり、移動機16において解釈・実行されると図11に示される説明ページ212を提供するように記述されている。また、ADF213はパッケージURLとしてJarファイル214のURL（“http://www.ccc.co.jp/shogi.jar”）を内包している。

【0047】

また、IPサーバ装置12の不揮発性メモリ12Aには、「星占い」なる名称のJava-APソフトウェア（以後、第2のJava-APソフトウェア）に対応する説明ファイル207、ADF209およびJarファイル210が記憶されているものとする。これらはIPサーバ装置12を管理するIPによって作成されている。これらのうち、説明ファイル207の内容は図12に示される通りであり、移動機16において解釈・実行されると図13に示される説明ページ208を提供するように記述されている。また、ADF209はパッケージURLとしてJarファイル210のURL（“http://www.ccc.co.jp/horoscope.jar”）を内包している。

【0048】

また、IPサーバ装置13の不揮発性メモリ13Aには、「電話帳ビューア」なる名称のJava-APソフトウェア（以後、第3のJava-APソフトウェア）に対応する説明ファイル202、ADF205およびJarファイル206が記憶されているものとする。これらはIPサーバ装置13およびIPサーバ装置14を管理するIPによって作成されている。これらのうち、説明ファイル202の内容は図14に示される通りであり、移動機16において解釈・実行さ

れると図15に示される説明ページ203を提供するように記述されている。ADF205は、APIDとして“0001”、ハッシュ値としてJarファイル206のハッシュ値、パッケージURLとしてJarファイル206のURL (“http://www.main.bbb.co.jp/viewer.jar”) を内包しており、IPサーバ装置13およびIPサーバ装置14を管理するIPに対してCAが付与した秘密鍵を用いて署名されている。

また、移動機16は第1～第3のJava-APソフトウェアをインストール可能な状態にあるものとする。

【0049】

(2-1) インストール動作

まず、Java-APソフトウェアを移動機16にインストールする場合の動作例について、Java-APソフトウェア毎に説明する。

【0050】

(2-1-1) 第1のJava-APソフトウェア

第1のJava-APソフトウェアのインストール動作は、ユーザが移動機16を操作し、説明ファイル211の取得を試みることから始まる。これにより、移動機16では、説明ファイル211のURL (“http://www.ccc.co.jp/mno.html”) をGETメソッドのパラメータとして含む要求メッセージtm12が生成される。この要求メッセージtm12は、図16に示されるように、移動機16から送信されIPサーバ装置12により受信される。IPサーバ装置12では、この要求メッセージtm12の内容に対応して説明ファイル211を内包した応答メッセージtm13が生成される。この応答メッセージtm13はIPサーバ装置12から送信され移動機16により受信される。移動機16では、ユーザに対して、説明ファイル211の内容に応じたUIが提供される。この結果、表示部16Cには、例えば図11に示すような説明ページ212が表示される。

【0051】

この説明ページ212を視たユーザが、説明ページ212内のアンカー212Aが押下されるよう移動機16を操作すると、移動機16では、図10の説明ファイル211に記述されたアンカータグ (“<A” で始まるタグ) のijam属性

に指定されている値が `id` 属性に指定されているオブジェクトタグ（“<OBJECT” で始まるタグ）が特定され、このオブジェクトタグの `data` 属性に指定されている URL（“<http://www.ccc.co.jp/shogi.jam>”）が抽出され、この URL で特定される ADF213 の送信を要求する内容の要求メッセージ `tm16` が生成される。この要求メッセージ `tm16` は移動機 16 から送信され IP サーバ装置 12 により受信される。IP サーバ装置 12 では、この要求メッセージ `tm16` の内容に対応して ADF213 を内包した応答メッセージ `tm17` が生成される。この応答メッセージ `tm17` は IP サーバ装置 12 から送信され移動機 16 により受信される。

【0052】

移動機 16 では、ADF213 の内容に基づいて第 1 の Java-AP ソフトウェアをインストール可能か否かが判定される。前述のように、移動機 16 は第 1 の Java-AP ソフトウェアをインストール可能な状態にあるから、移動機 16 では第 1 の Java-AP ソフトウェアをインストール可能と判定される。

【0053】

次に、移動機 16 では、ADF213 が不揮発性メモリ 16D1 に書き込まれる。また、移動機 16 では、ADF213 からパッケージ URL（“<http://www.ccc.co.jp/shogi.jar>”）が抽出され、このパッケージ URL で特定される Jar ファイル 214 の送信を要求する内容の要求メッセージ `tm18` が生成される。この要求メッセージ `tm18` は移動機 16 から送信され IP サーバ装置 12 により受信される。IP サーバ装置 12 では、この要求メッセージ `tm18` の内容に対応して Jar ファイル 214 を内包した応答メッセージ `tm19` が生成される。この応答メッセージ `tm19` は IP サーバ装置 12 から送信され移動機 16 により受信される。移動機 16 では Jar ファイル 214 が不揮発性メモリ 16D1 に書き込まれ、第 1 の Java-AP ソフトウェアのインストールが完了する。

なお、移動機 16 において第 1 の Java-AP ソフトウェアをインストール可能ではないと判断された場合、移動機 16 の状態は、ADF213 の取得を開始する前の状態に戻る。

【0054】

(2-1-2) 第2のJava-APソフトウェア

第2のJava-APソフトウェアのインストール動作は、ユーザが移動機16を操作し、説明ファイル207またはリストファイル200の取得を試みることから始まる。説明ファイル207の取得を試みることから始まる動作はリストファイル200の取得を試みることから始まる動作のサブセットになっていることから、ここでは、リストファイル200の取得を試みることから始まる動作のみについて説明する。

【0055】

図17に示されるように、移動機16では、リストファイル200のURL (“http://www.aaa.co.jp/def.html”) をGETメソッドのパラメータとして含む要求メッセージtm20が生成される。この要求メッセージtm20は移動機16から送信され管理サーバ装置18により受信される。管理サーバ装置18では、この要求メッセージtm20の内容に対応してリストファイル200を内包した応答メッセージtm21が生成される。この応答メッセージtm21は管理サーバ装置18から送信され移動機16により受信される。移動機16では、応答メッセージtm21の受信を契機として、応答メッセージtm21内のリストファイル200がHTMLに従って解釈され、移動機16のユーザに対して、リストファイル200の内容に応じたUIが提供される。この結果、移動機16の表示部16Cには、例えば図9に示すようなリストページ201が表示される。

【0056】

このリストページ201を視たユーザが、リストページ201内の選択肢201Bが押下されるように移動機16を操作すると、移動機16では、選択肢201Bに対応付けられているURL (“http://www.ccc.co.jp/jkl.html”) をGETメソッドのパラメータとして含む要求メッセージtm22が生成される。この要求メッセージtm22は移動機16から送信されIPサーバ装置12により受信される。IPサーバ装置12では、この要求メッセージtm22の内容に対応して説明ファイル207を内包した応答メッセージtm23が生成される。この応答メッセージtm23はIPサーバ装置12から送信され移動機16により

受信される。移動機16では、ユーザに対して、説明ファイル207の内容に応じたUIが提供される。この結果、表示部16Cには、例えば図13に示すような説明ページ208が表示される。

【0057】

この説明ページ208を視たユーザが、説明ページ208内のアンカー208Aが押下されるよう移動機16を操作すると、移動機16では、図12の説明ファイル207に記述されたアンカータグ（“<A”で始まるタグ）の*i j a m*属性に指定されている値が*i d*属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）が特定され、このオブジェクトタグの*d a t a*属性に指定されているURL（“<http://www.ccc.co.jp/horoscope.jam>”）が抽出され、このURLで特定されるADF209の送信を要求する内容の要求メッセージ*t m 2 6*が生成される。この要求メッセージ*t m 2 6*は移動機16から送信されIPサーバ装置12により受信される。IPサーバ装置12では、この要求メッセージ*t m 2 6*の内容に対応してADF209を内包した応答メッセージ*t m 2 7*が生成される。この応答メッセージ*t m 2 7*はIPサーバ装置12から送信され移動機16により受信される。

【0058】

移動機16では、ADF209の内容に基づいて第2のJava-APソフトウェアをインストール可能か否かが判定される。前述のように、移動機16は第2のJava-APソフトウェアをインストール可能な状態にあるから、移動機16では第2のJava-APソフトウェアをインストール可能と判定される。

【0059】

次に、移動機16では、ADF209が不揮発性メモリ16D1に書き込まれる。また、移動機16では、ADF209からパッケージURL（“<http://www.ccc.co.jp/horoscope.jar>”）が抽出され、このパッケージURLで特定されるJarファイル210の送信を要求する内容の要求メッセージ*t m 2 8*が生成される。この要求メッセージ*t m 2 8*は移動機16から送信されIPサーバ装置12により受信される。IPサーバ装置12では、この要求メッセージ*t m 2 8*の内容に対応してJarファイル210を内包した応答メッセージ*t m 2 9*が生成

される。この応答メッセージ `tm29` は IPサーバ装置 12 から送信され移動機 16 により受信される。移動機 16 では `Jar` ファイル 210 が不揮発性メモリ 16D1 に書き込まれ、第2の `Java-AP` ソフトウェアのインストールが完了する。

なお、移動機 16 において、第2の `Java-AP` ソフトウェアをインストール可能ではないと判断された場合、移動機 16 の状態は、`ADF209` の取得を開始する前の状態に戻る。

【0060】

(2-1-3) 第3の `Java-AP` ソフトウェア

第3の `Java-AP` ソフトウェアのインストール動作は、ユーザが移動機 16 を操作し、説明ファイル 202 またはリストファイル 200 の取得を試みることから始まる。説明ファイル 202 の取得を試みることから始まる動作はリストファイル 200 の取得を試みることから始まる動作のサブセットになっていることから、説明ファイル 202 の取得を試みることから始まる動作についての説明を省略する。

【0061】

図 18 に示されるように、リストファイル 200 の取得を試みることから始まる動作において、移動機 16 が応答メッセージ `tm21` を受信し、例えば図 9 に示すようなリストページ 201 が表示されるまでは図 17 に示す動作と同一の動作が行われる。このリストページ 201 を視たユーザが、リストページ 201 内の選択肢 201A が押下されるように移動機 16 を操作すると、移動機 16 では、選択肢 201A に対応付けられている URL ("`http://www.main.bbb.co.jp/ghi.html`") を `GET` メソッドのパラメータとして含む要求メッセージ `tm32` が生成される。この要求メッセージ `tm32` は移動機 16 から送信され IPサーバ装置 13 により受信される。IPサーバ装置 13 では、この要求メッセージ `tm32` の内容に対応して説明ファイル 202 を内包した応答メッセージ `tm33` が生成される。この応答メッセージ `tm33` は IPサーバ装置 13 から送信され移動機 16 により受信される。移動機 16 では、ユーザに対して、説明ファイル 202 の内容に応じた UI が提供される。この結果、表示部 16C には、例えば

図15に示すような説明ページ203が表示される。

【0062】

この説明ページ203を視たユーザが、説明ページ203内のアンカー203Aが押下されるよう移動機16を操作すると、移動機16では、図14の説明ファイル202に記述されたアンカータグ（“<A”で始まるタグ）の*i j a m*属性に指定されている値が*i d*属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）が特定され、このオブジェクトタグの*d a t a*属性に指定されているURL（“<http://www.aaa.co.jp/abc.sdf>”）が抽出され、このURLで特定されるSDF204の送信を要求する内容の要求メッセージ*t m 3 4*が生成される。この要求メッセージ*t m 3 4*は移動機16から送信され管理サーバ装置18により受信される。管理サーバ装置18では、この要求メッセージ*t m 3 4*の内容に対応してSDF204を内包した応答メッセージ*t m 3 5*が生成される。この応答メッセージ*t m 3 5*は管理サーバ装置18から送信され、ゲートウェイサーバ装置17及び移動パケット通信網15を介して移動機16により受信される。管理サーバ装置18とゲートウェイサーバ装置17との間の通信路は専用線であり、ゲートウェイサーバ装置17はセキュリティの確保された移動パケット通信網15に直接的に接続されていることから、移動機16に受信されるまでにSDF204が改竄される虞は無い。

【0063】

移動機16において、SDF204は不揮発性メモリ16Dの不揮発性メモリ16D1に書き込まれる。また、移動機16では、SDF204からAPIID（“0001”）とADF-URL（“<http://www.main.bbb.co.jp/viewer.jam>”）と公開鍵が抽出され、このADF-URLで特定されるADF205の送信を要求する内容の要求メッセージ*t m 3 6*が生成される。この要求メッセージ*t m 3 6*は移動機16から送信されIPサーバ装置13により受信される。IPサーバ装置13では、この要求メッセージ*t m 3 6*の内容に対応してADF205を内包した応答メッセージ*t m 3 7*が生成される。この応答メッセージ*t m 3 7*はIPサーバ装置13から送信され移動機16により受信される。

【0064】

移動機16ではSDF204から抽出された公開鍵を用いてADF205の正当性が判断される。前述のように、SDF204に内包されている公開鍵はADF205への署名の際に用いた秘密鍵と対応していることから、IPサーバ装置13内あるいはIPサーバ装置13から移動機16への通信経路においてADF205が変更されていない限り、ADF205が正当であると判断される。

【0065】

ADF205が正当であると判断されると、移動機16では、SDF204から抽出されたAPIDとADF205に内包されているAPIDとが比較される。前述のように、IPサーバ装置13におけるADF205にはSDF204内のAPIDと一致するAPIDが記述されるように定められていることから、記述ミス等が無い限り、SDF204から抽出されたAPIDとADF205に内包されているAPIDは一致する。

【0066】

APIDが一致すると、移動機16では、ADF205の内容に基づいて第3のJava-APソフトウェアをインストール可能か否かが判定される。前述のように、移動機16は第3のJava-APソフトウェアをインストール可能な状態にあるから、移動機16では第3のJava-APソフトウェアをインストール可能と判定される。

【0067】

次に、移動機16では、ADF205が不揮発性メモリ16D1に書き込まれる。また、移動機16では、ADF205からハッシュ値とパッケージURL（“http://www.main.bbb.co.jp/viewer.jar”）が抽出され、このパッケージURLで特定されるJarファイル206の送信を要求する内容の要求メッセージtm38が生成される。この要求メッセージtm38は移動機16から送信されIPサーバ装置13により受信される。IPサーバ装置13では、この要求メッセージtm38の内容に対応してJarファイル206を内包した応答メッセージtm39が生成される。この応答メッセージtm39はIPサーバ装置13から送信され移動機16により受信される。

【0068】

移動機16ではJarファイル206と所定のハッシュ関数とを用いてハッシュ値が算出され、このハッシュ値とADF205から抽出されたハッシュ値とが比較される。前述のように、ADF205には当該ADF205に対応するJarファイルのハッシュ値が記述されるように定められていることから、記述ミス等がない限り、両ハッシュ値は一致する。両ハッシュ値が一致すると、移動機16では、Jarファイル206が不揮発性メモリ16D1に書き込まれ、第3のJava-APソフトウェアのインストールが完了する。

【0069】

なお、移動機16においてADF205が正当でないと判断された場合や、SDF204から抽出されたAPIDとADF205に内包されているAPIDが不一致の場合、第3のJava-APソフトウェアをインストール可能ではないと判断された場合、算出したハッシュ値とADF205から抽出されたハッシュ値とが不一致の場合には、移動機16の状態は、SDF204の取得を開始する前の状態に戻る。

【0070】

(2-2) Java-APソフトウェアが起動されている時の移動機16の挙動
次に、Java-APソフトウェアが起動されている時の移動機16の挙動について説明する。

(2-2-1) 第1のJava-APソフトウェア

上述したインストール動作により移動機16にインストールされた第1のJava-APソフトウェアが、JAMが実現された移動機16において起動され、当該ソフトウェアに対応した機能（以後、第1のJava-AP）が移動機16内に実現されたときの移動機16の挙動について説明する。

【0071】

第1のJava-APが使用しようとするAPIが非トラステッドAPIの場合、当該APIの使用はJAMにより許可される。したがって、第1のJava-APは当該APIを使用することができる。

また、第1のJava-APが使用しようとするAPIがトラステッドAPIの場合、JAMは当該Java-APに対応するSDFが不揮発性メモリ16D

に記憶されているか否かを調べる。そのようなSDFは不揮発性メモリ16Dに記憶されていないから、JAMは第1のJava-APによる当該APIの使用を禁止する。したがって、第1のJava-APは当該APIの使用することができない。

【0072】

(2-2-2) 第2のJava-APソフトウェア

移動機16にインストールされた第2のJava-APソフトウェアが、JAMが実現された移動機16において起動され、当該ソフトウェアに対応した機能が移動機16内に実現されたときの移動機16の挙動は、第1のJava-APソフトウェアが起動されている時の移動機16の挙動と同様となる。

【0073】

(2-2-3) 第3のJava-APソフトウェア

移動機16にインストールされた第3のJava-APソフトウェアが、JAMが実現された移動機16において起動され、当該ソフトウェアに対応した機能（以後、第3のJava-AP）が移動機16内に実現されたときの移動機16の挙動について説明する。

【0074】

第3のJava-APが使用しようとするAPIが非トラステッドAPIの場合当該APIの使用はJAMにより許可される。したがって、第3のJava-APは当該APIを使用することができる。

第3のJava-APが使用しようとするAPIがトラステッドAPIの場合、移動機16の挙動は使用するAPIに依存する。以下、使用するAPI毎に移動機16の挙動を説明する。

【0075】

(2-2-3-1) getPhoneList()

“getPhoneList()”はトラステッドAPIであるから、当該APIの使用の可否は、不揮発性メモリ16Dに記憶されているSDF204内のポリシー情報に基づいてJAMにより決定される。このポリシー情報の内容は図7に示される通りであることから、“getPhoneList()”の使用がJAMにより許可される。した

がって、第3のJava-APは“getPhoneList()”を使用することができる。
つまり、第3のJava-APは電話帳データを読み出すことができる。

【0076】

(2-2-3-2) getCallHistory()

“getCallHistory()”はトラステッドAPIであるから、当該APIの使用の可否はSDF204内のポリシー情報に基づいてJAMにより決定される。このポリシー情報の内容は図7に示される通りであることから、“getCallHistory()”の使用がJAMにより禁止される。したがって、第3のJava-APは“getCallHistory()”を使用することができない。つまり、第3のJava-APは発着信履歴データを読み出すことができない。

【0077】

(2-3) 第3のJava-APソフトウェアの変更後の動作

次に、IPサーバ装置13およびIPサーバ装置14を管理するIPが第3のJava-APソフトウェアの配信形態や内容を変更した場合の本システム動作について説明する。ただし、ここでの変更は、第3のJava-APソフトウェアの改善等を目的としたJarファイル206の内容の変更と、IPサーバ装置13の負荷の軽減等を目的とした配信形態の変更とを含む。後者の変更を達成するために、IPサーバ装置13およびIPサーバ装置14を管理するIPは、図19に示すように、変更後のJarファイル206（以後、Jarファイル215）をIPサーバ装置14の不揮発性メモリ14Aに記憶させ、このJarファイル215に対応するようにADF205の内容を変更してADF216としている。変更後の第3のJava-APソフトウェアの配信に必要な作業は以上の通りであり、管理サーバ装置18を管理する通信事業者が行うべき作業は存在しない。

【0078】

このような変更の後の第3のJava-APソフトウェアのインストール動作は、図20に示す通りとなる。この図に示す動作が図18に示す動作と相違し始めるのは、IPサーバ装置13において、ADF205を内包した応答メッセージtm37ではなく、ADF216を内包した応答メッセージtm47を生成し

てからである。なお、両図において、応答メッセージ t_{m47} は応答メッセージ t_{m37} 、要求メッセージ t_{m48} は要求メッセージ t_{m38} 、応答メッセージ t_{m49} は応答メッセージ t_{m39} に対応している。

【0079】

IPサーバ装置13において応答メッセージ t_{m47} を生成して以降の動作が、図18に示す動作と本質的に異なるのは、ADF216およびJarファイル215が処理の対象となる点と、ADF216に内包されているパッケージURL (“<http://www.sub.bbb.co.jp/viewer.jar>”) で特定されるJarファイル215の送信を要求する内容の要求メッセージ t_{m48} が移動機16にて生成される点と、この要求メッセージ t_{m48} が移動機16から送信されIPサーバ装置14により受信される点と、IPサーバ装置14においてJarファイル215を内包した応答メッセージ t_{m49} が生成される点と、この応答メッセージ t_{m49} がIPサーバ装置14から送信され移動機16により受信される点のみである。

【0080】

(3) 変形例

上述した配信システムでは、移動機は、秘密鍵による署名データと公開鍵とを用いてSDFとADFの作成者との対応関係の正当性を確認するようにしたが、システムに要求されるセキュリティレベルによっては、SDFに公開鍵を内包させず、IPサーバ装置においてはADFに対する秘密鍵を用いた署名を行わず、かつ移動機においては当該確認処理を省略する、という形態とし、移動機およびIPサーバ装置における処理量や、移動機と管理サーバ装置およびIPサーバ装置との間の通信量を低減するようにしてもよい。

【0081】

また、上述した配信システムでは、Jarファイルのハッシュ値を当該Jarファイルに対応するADFに内包させる一方、移動機において生成し、両者を比較し、JarファイルとADFとの対応関係の正当性を確認するようにしたが、システムに要求されるセキュリティレベルによっては、ADFにハッシュ値を内包させずに当該確認処理を省略する形態とし、移動機およびIPサーバ装置にお

ける処理量や移動機とIPサーバ装置との間の通信量を低減するようにしてもよい。

【0082】

また、上述した配信システムでは、トラステッドJava-APに固有のAPIDを使用してSDFとADF（およびJarファイル）との対応が正当であるか否かを判定するようにしたが、トラステッドJava-APを提供する情報提供事業者に固有のCIDを用いてSDFとADF（およびJarファイル）との対応が正当であるか否かを判定するようにしてもよい。また、システムに要求されるセキュリティレベルによっては、APIDやCIDを用いた判定を省略するようにしてもよい。

【0083】

また、上述した配信システムではドメインネームを用いてサーバを指定するようにしたが、IPアドレスを用いてサーバを指定するようにしてもよい。

また、移動機において、SDFの送信元のサーバ装置のドメインネームを予め設定された文字列と比較し、信頼できる機関が管理するサーバ装置のドメインネームである場合にのみ、SDFを正当と認める態様としてもよい。この態様では、比較対象の文字列（例えば、通信事業者のドメインネームを示す文字列）は移動機のROMまたは不揮発性メモリに予め格納されることになる。ROMに予め格納する態様では、文字列の書き換えが不可能であるから、より高いセキュリティを確保できる。また、不揮発性メモリに予め格納する態様では、移動機の売買後に信頼できる機関を格納することができるので、ユーザおよび信頼できる機関に対して優れた利便性を提供することができる。

【0084】

また、上述した配信システムでは、SDFの配信に使用する通信路を提供する通信事業者を信頼できる機関として高いセキュリティを確保するようにしたが、本発明は通信路の提供が信頼できる機関により為されていない態様をも技術的範囲に含む。例えば、信頼できる機関と移動機とを暗号化通信路により接続し、この通信路を介して信頼できる機関がSDFを配信するようにしてもよい。また、通信路のセキュリティが確保されていなくても、SDFを暗号化した後に配信し

、移動機においてSDFを復号するようにすれば、ある程度のセキュリティを確保してSDFを配信することができる。

【0085】

上述した配信システムでは、HTTPに従ってファイルを送受するようにしたが、HTTPSを使用し、より高いセキュリティを確保するようにシステムを變形してもよい。

また、上述した配信システムにおいて、信頼できる機関がIPとなってよいこと、すなわち、管理サーバ装置がIPサーバ装置を兼ねるようにしてもよいことは言うまでもない。

【0086】

さらに、上述した配信システムでは、Java-APによる利用を制限する対象としてAPIを挙げたが、本発明はこれに限定されるものではなく、任意の資源（リソース）を対象とすることができる。ここでいう資源はハードウェア資源であってもよいし、後述するネットワーク資源やソフトウェア資源であってもよい。ハードウェア資源としては、メモリやスピーカ、マイク、赤外線コントローラ、LED（Light Emitting Diode）等の移動機が備え得るものや移動機と共働し得るUIM（User Identity Module）やSIM（Subscriber Identity Module）等の外部機器なども挙げられる。

【0087】

次にネットワーク資源について説明する。前述したように、移動機は移動通信網との間で無線通信を行う。この無線通信時には、移動機は、移動通信網により提供される無線チャネル等の無線資源を使用する。この無線資源はネットワーク資源の一種である。また、移動機は無線資源が属する通信プロトコルレイヤよりも高位の通信プロトコルレイヤにおいて、パケットの伝送路や回線接続の通信路などの通信資源を使用する。このような通信資源もネットワーク資源の一種である。

【0088】

次にソフトウェア資源について説明する。ソフトウェア資源としては、APIやクラス、パッケージ等が挙げられる。ソフトウェア資源が提供する機能は様々

であるが、典型的な機能として、暗号演算などの演算処理機能や、Webブラウザ等の他のアプリケーションとの間でデータを送受したりする機能などが挙げられる。また、本発明は、上記外部機器が有するソフトウェア資源をも利用の制限対象とする態様を技術的範囲に含む。

【0089】

ところで、Java-A Pによるハードウェア資源やネットワーク資源の利用は、ソフトウェア資源を利用して行われるのが一般的である。上述した配信システムにおける移動機も、ハードウェア資源やネットワーク資源を利用するためのソフトウェア資源を有しており、このようなソフトウェア資源の利用を制限することにより、間接的に、ハードウェア資源やネットワーク資源の利用を制限している。このように、間接的な制限の形態としたことにより、多様なソフトウェア資源を用意すれば、Java-A PのうちのトラステッドJava-A Pについてのみ、自他のJava-A Pの権限を変更する権限を与える、またはダウンロード元のサーバ装置としか通信することができないという制限を外す、あるいはメモリの特定の記憶領域に対してアクセスできるようにするといった、複数の資源の制限を細かく変更しなければ実現できないようなことまで容易に指定できるようになる。なお、移動機内部のソフトウェア資源の利用を制限して上記外部機器のソフトウェア資源の利用を間接的に制限する態様も本発明の技術的範囲に含まれる。

【0090】

なお、パーミッションの表現方法としては、一つの資源と一つのフラグ（許可／禁止）とを対応付けるようにしてもよいし、複数の資源のパーミッションを一つの情報で示すようにしてもよい。

【0091】

また、本発明では、複数の利用の種類を持つ資源について、利用を許可（あるいは禁止）する種類を示すようにパーミッションを設定することも可能である。この場合、移動機において、より木目細かな制御が実現される。例えば、メモリには読み出しと書き込みの2つの利用形態（利用の種類）があるから、非トラステッドJava-A Pには読み出しでしか利用されないが、トラステッドJava

a-A Pには読み出し及び書き込みの両方で利用され得るようにすることもできる。また、例えば、1つのパケット伝送路を複数のアプリケーションが共用可能な移動機において、パケット伝送路を利用する権限を有するJ a v a-A Pが起動されている間にW e bブラウザ等が起動された場合、当該J a v a-A Pが「パケット伝送路の利用を排他的に行う」ことを許可されていないJ a v a-A PであればW e bブラウザ等によるパケット伝送路の共用を排除することはできないが、「パケット伝送路の利用を排他的に行う」ことを許可されているJ a v a-A Pであればパケット伝送路を占有して使用することができる、といった制御が可能となる。さらに、この例を変形することで、ある種のパーミッションを与えられたJ a v a-A Pはユーザに許可を求めることなくパケット通信路を排他的に利用することが可能であり、別のパーミッションを与えられたJ a v a-A Pはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用するためにはユーザの許可を得ることが必要であり、さらに別のパーミッションを与えられたJ a v a-A Pはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用することは不可能であり、さらに別のパーミッションを与えられたJ a v a-A Pはユーザの許可を得て初めてパケット通信路を利用することが可能であり、さらに別のパーミッションを与えられたJ a v a-A Pはパケット通信路を利用することすらできない、といった制御も可能となる。この例から明らかなように、本発明における「利用の種類」には、資源を利用する際に経る手順の種類（ユーザの許可を得る手順／ユーザの許可を得ない手順）も含まれる。

【0092】

また、上述した配信システムでは全ての移動機に対して同一のリストページが提供されるが、移動機毎に異なるリストページを提供するようにしてもよい。

【0093】

また、上述の配信システムでは、J a v a-A Pの実行時にJ a v a-A Pの挙動を制限するようにしたが、I Pサーバ装置に格納されているJ a rファイルにポリシー情報を内包させ、J a rファイルのダウンロード時に、移動機において、このポリシー情報とS D F中とのポリシー情報とを比較し、両者が一致しな

い場合には、当該 Jar ファイルに対応する Java-AP を起動できないように、あるいは当該 Jar ファイルを含む Java-AP ソフトウェアをインストールできないようにしてもよい。もちろん、両ポリシー情報の一致する項目についてのパーミッションのみを有効とするようにしてもよい。

【0094】

また、通信事業者が CA により付与された自身の秘密鍵を用いて SDF に署名してから SDF を配信し、移動機において CA が通信事業者に付与した公開鍵を用いて SDF の署名を検証するようにしてもよい。もちろん、通信事業者の公開鍵は予め移動機に格納されていなければならない。公開鍵は予め移動機に格納する方法としては、通信により配信し不揮発性メモリに書き込んでおく方法、ROM に書き込んだ後に移動機を販売する方法などが考えられる。

また、上述の配信システムではソフトウェアは移動機へ配信されるが、本発明の技術的範囲には、移動機以外の端末装置へ配信する態様も含まれる。

【0095】

【発明の効果】

以上説明したように、本発明によれば、端末装置では、取得したセキュリティ記述ファイルに示される権限に応じた挙動が当該セキュリティ記述ファイルに対応するアプリケーションに許可される。したがって、多様なアプリケーションを提供することができる。さらに、権限を示す情報は管理サーバ装置からセキュリティが確保された上で端末装置へ送信されるから、権限が第三者により改竄される虞もない。また、依存関係を有するアプリケーション記述ファイルおよび実体ファイルを管理サーバ装置に格納する必要はないことから、IP の自由度が制限されることもない。

【図面の簡単な説明】

【図1】 本発明の実施の一形態に係る配信システムの構成を示すブロック図である。

【図2】 同システムに特有のADFのデータ構成を示す概念図である。

【図3】 同システムを構成する移動機16の構成を示すブロック図である。

【図 4】 同移動機 16 の機能構成を示す概念図である。

【図 5】 同移動機 16 が J a v a - A P ソフトウェアをダウンロードしインストールする処理の流れを示すフローチャートである。

【図 6】 同システムにおいて管理サーバ装置 18 に格納されている S D F のデータ構成を示す概念図である。

【図 7】 同 S D F に内包されるポリシー情報の内容を示す概念図である。

【図 8】 同配信システムの動作を説明するためのブロック図である。

【図 9】 同配信システムにて配信されるリストページを示す図である。

【図 10】 同配信システムを構成する I P サーバ装置 12 が格納している説明ファイルの内容を示す図である。

【図 11】 同配信システムにて配信される説明ページを示す図である。

【図 12】 同 I P サーバ装置 12 が格納している説明ファイルの内容を示す図である。

【図 13】 同配信システムにて配信される説明ページを示す図である。

【図 14】 同配信システムを構成する I P サーバ装置 13 が格納している説明ファイルの内容を示す図である。

【図 15】 同配信システムにて配信される説明ページを示す図である。

【図 16】 同配信システムの動作を説明するためのシーケンス図である。

【図 17】 同配信システムの動作を説明するためのシーケンス図である。

【図 18】 同配信システムの動作を説明するためのシーケンス図である。

【図 19】 同配信システムの他の動作を説明するためのブロック図である。

【図 20】 同配信システムの他の動作を説明するためのシーケンス図である。

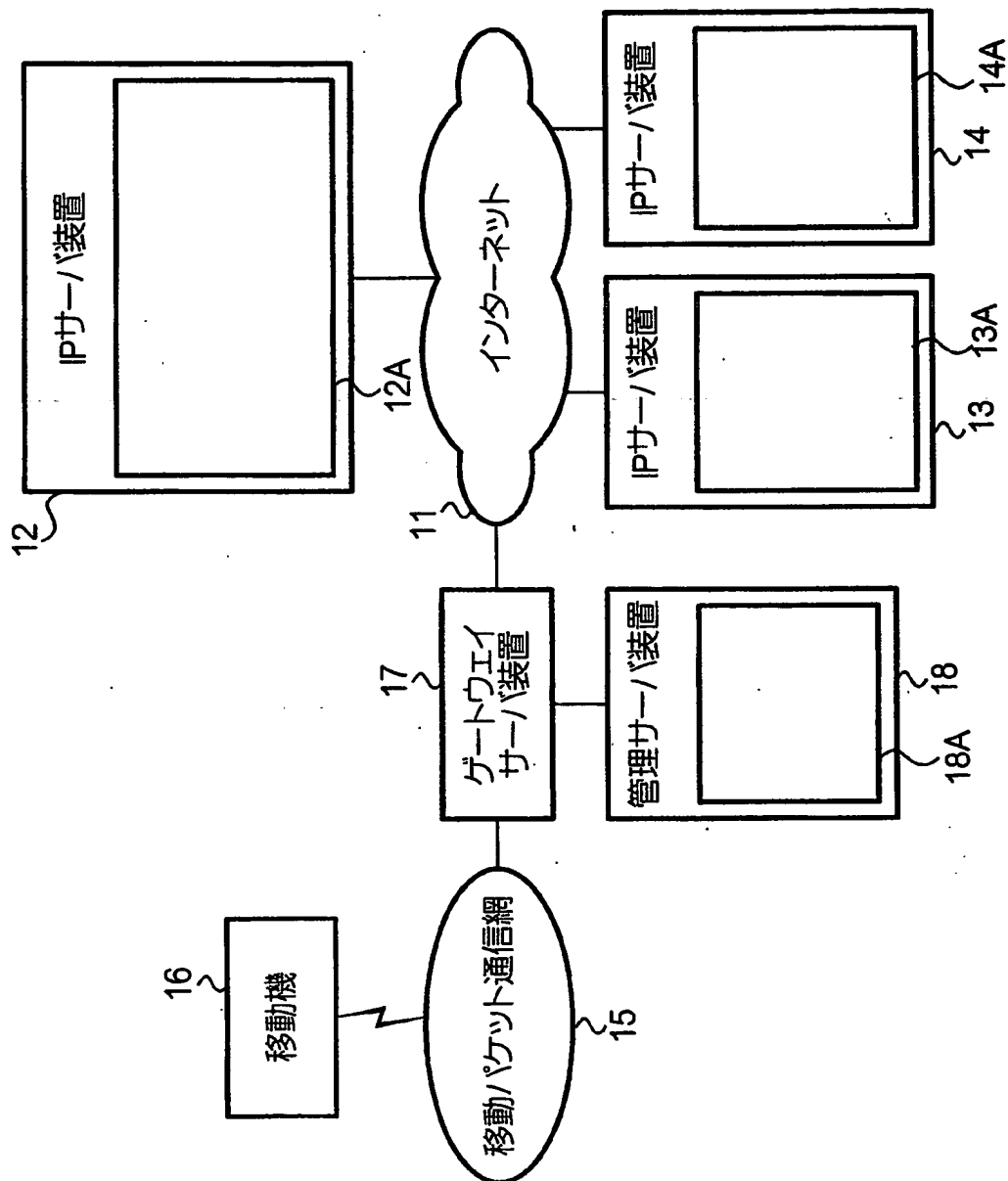
【符号の説明】

- 1 1 インターネット
- 1 2、1 3、1 4 I P サーバ装置
- 1 5 移動パケット通信網
- 1 6 移動機

1 7 ゲートウェイサーバ装置
1 8 管理サーバ装置
1 6 D、1 2 A、1 3 A、1 4 A、1 8 A 不揮発性メモリ
1 6 A R O M
1 6 B C P U
1 6 C 表示部
1 6 E R A M
1 6 F 通信部
1 6 G 操作部

【書類名】 図面

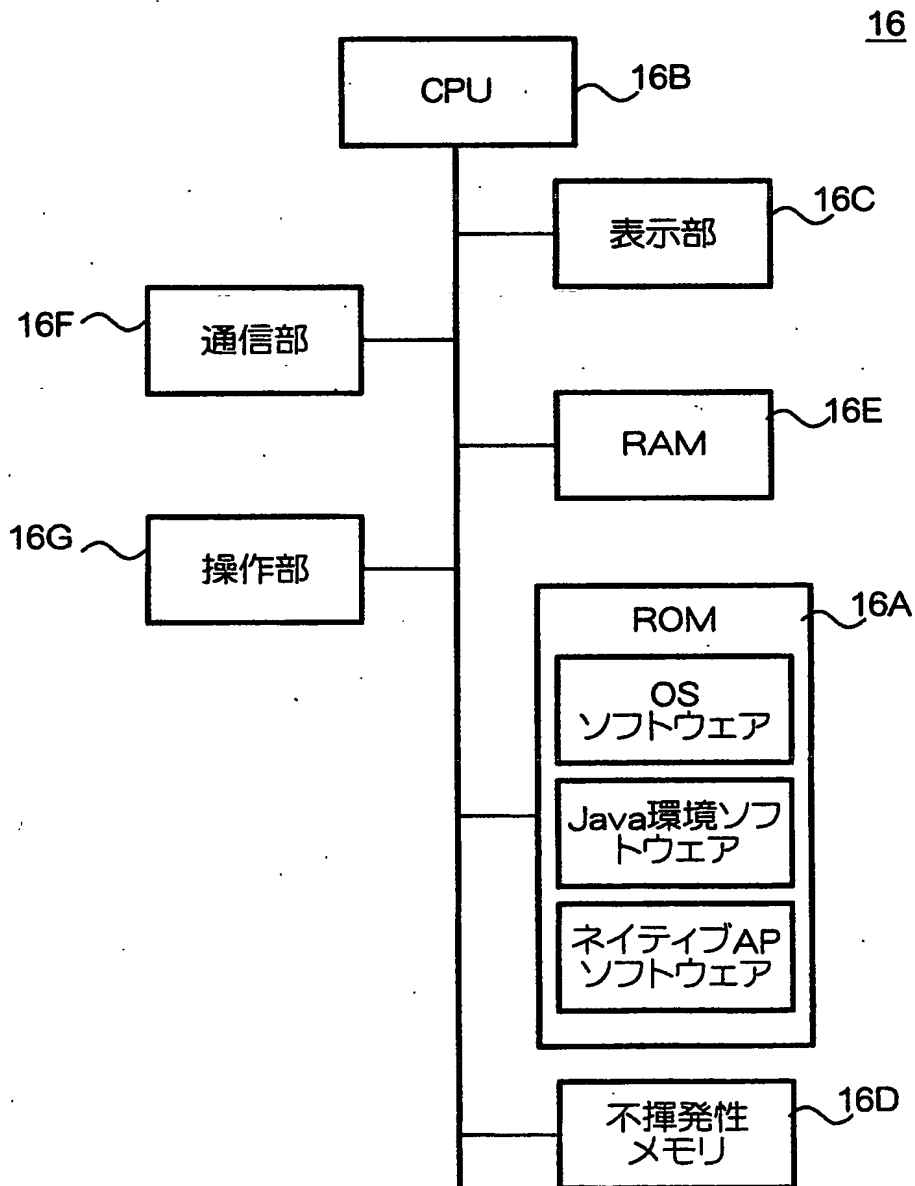
【図 1】



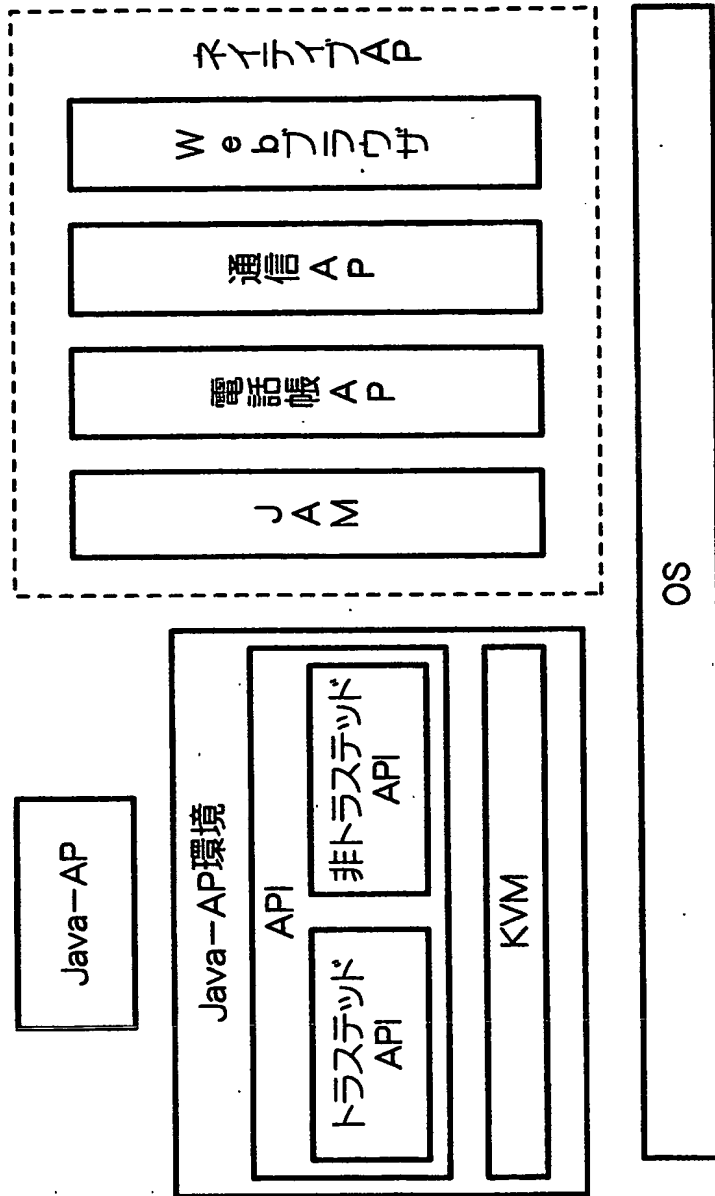
【図 2】



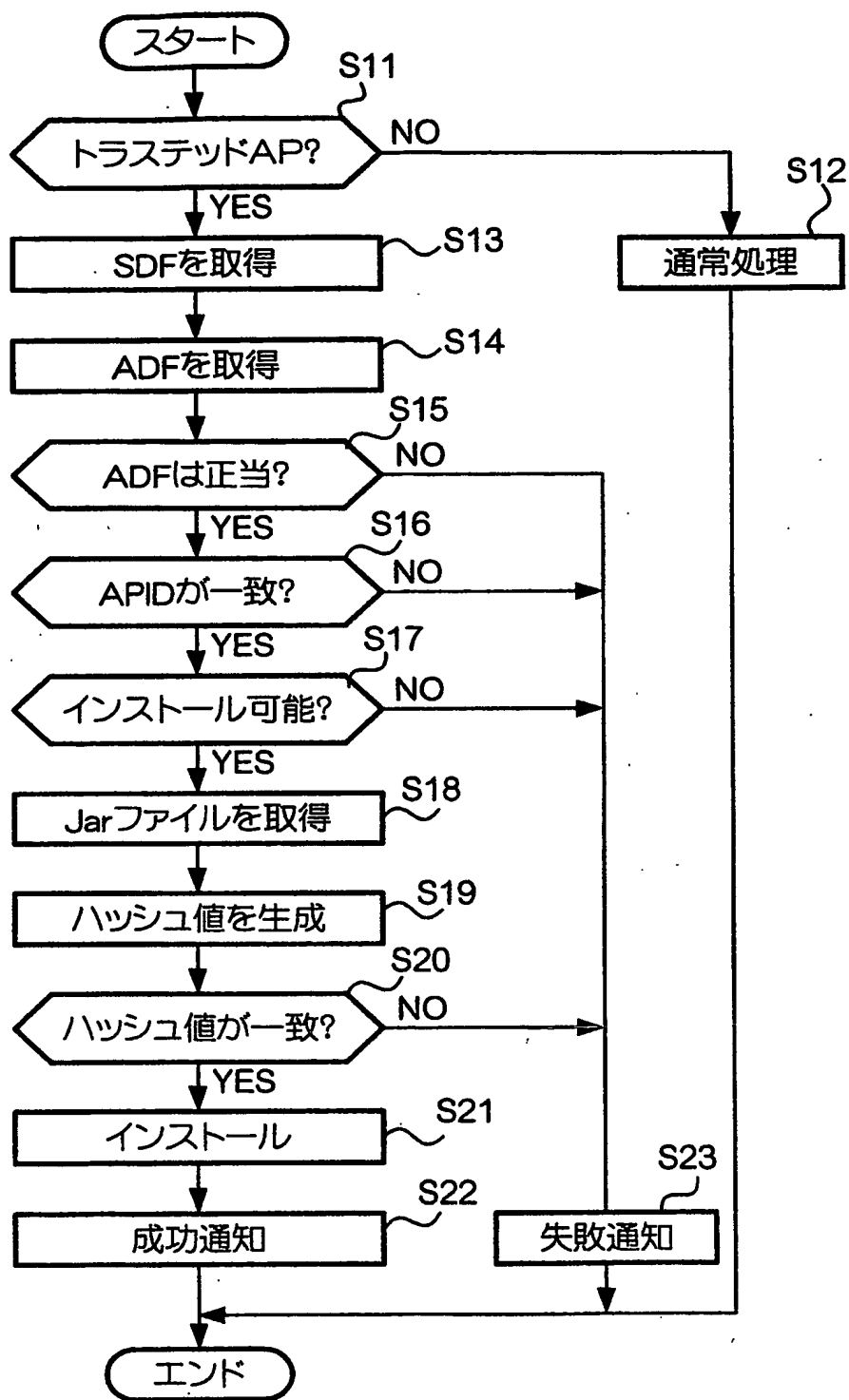
【図 3】



【図 4】



【図5】



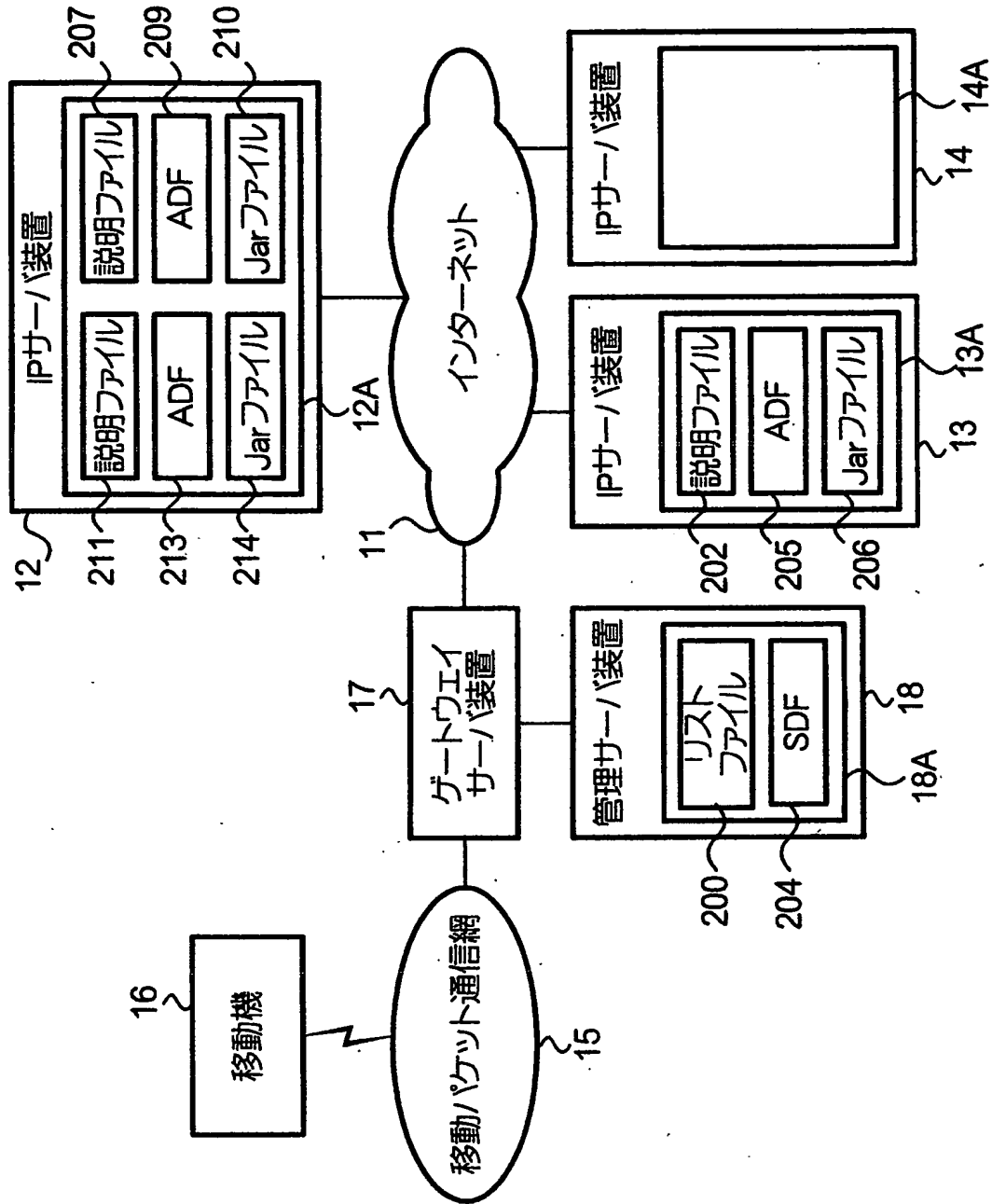
【図 6】

APIID	ポリシー情報	ADF-URL	公開鍵
-------	--------	---------	-----

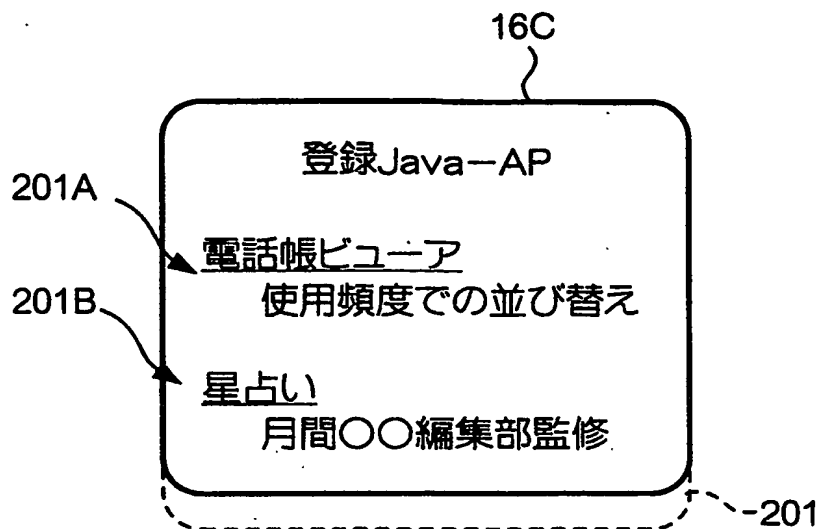
【図 7】

トラステッドAPI	パーミッション
getPhoneList()	○
getCallHistory()	×
getMsStatus()	○

【図 8】



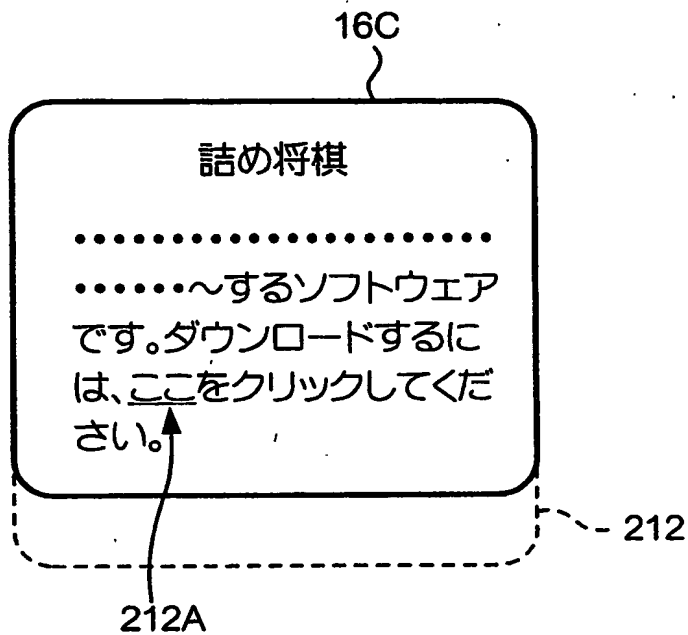
【図 9】



【図 1 0】

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/horoscope.jam">
詰め将棋
</OBJECT>
  ~するソフトウェアです。ダウンロードするには
  <A ijam="#application.declaration">ここ</A>
をクリック。
```

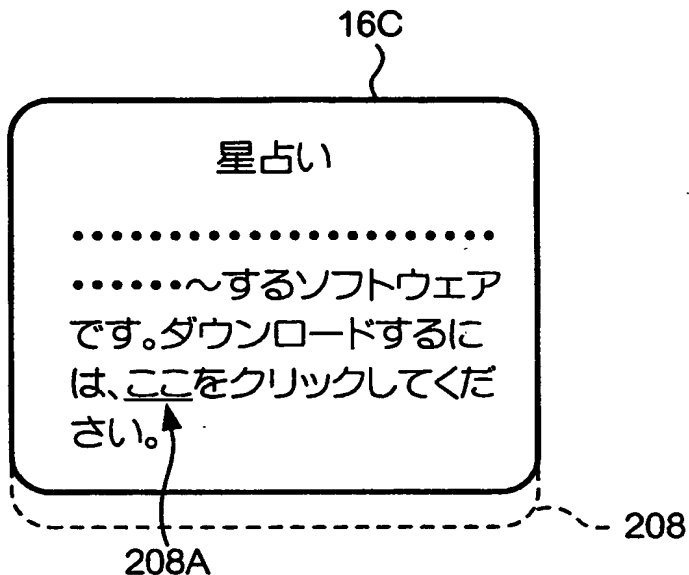

【図 1 1】



【図 1 2】

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/viewer.jam">
星占い
</OBJECT>
  ~するソフトウェアです。ダウンロードするには
  <A ijam="#application.declaration">ここ</A>
  をクリック。
```

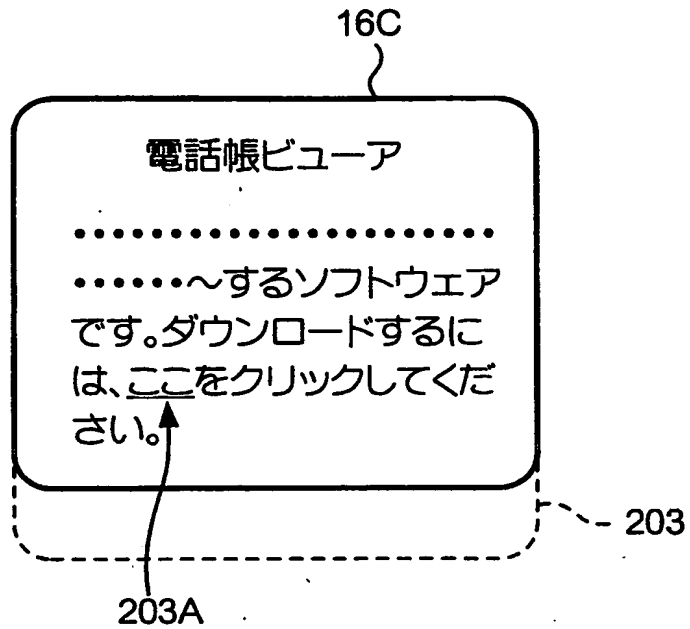
【図 13】



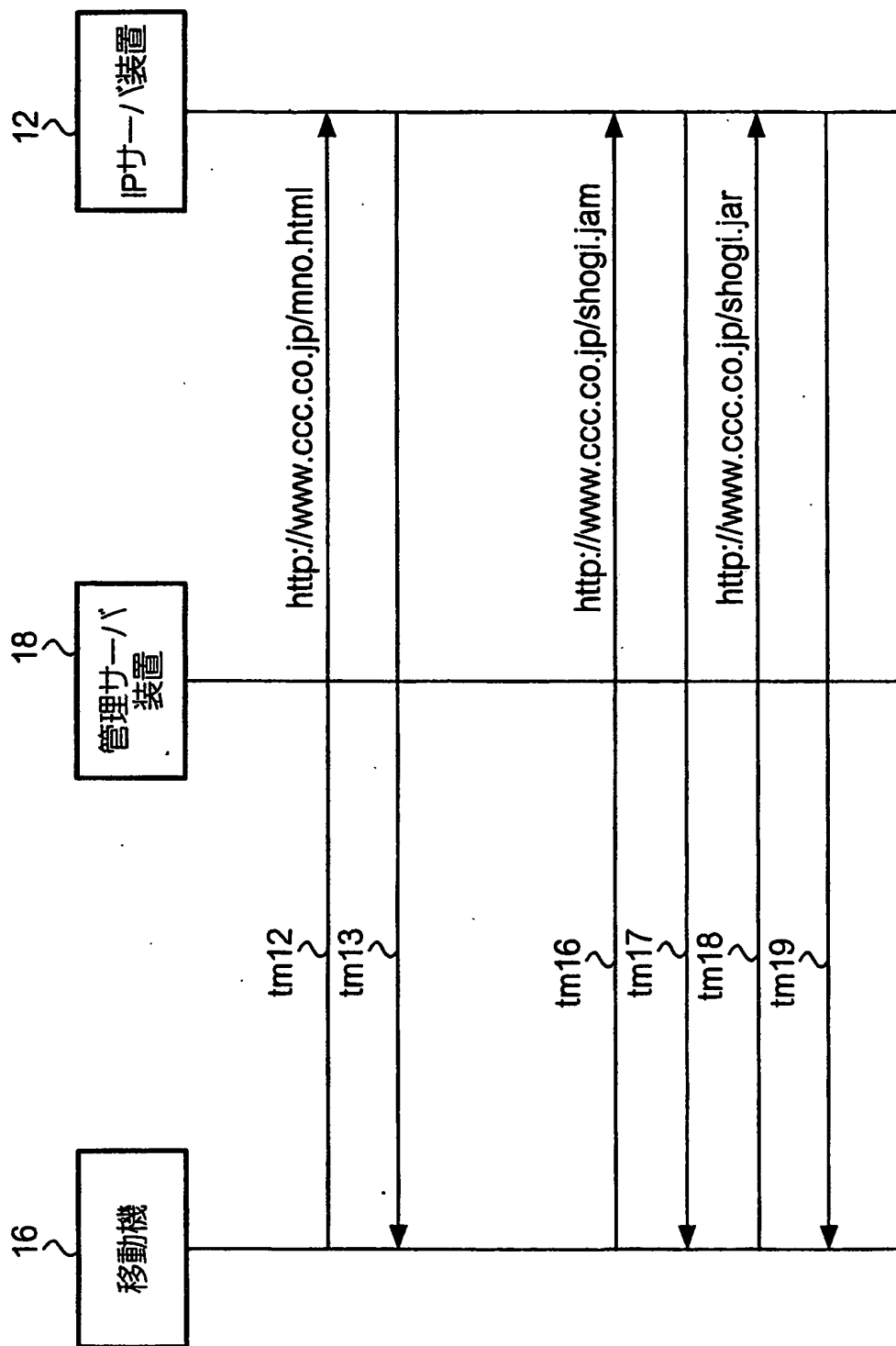
【図 14】

```
<OBJECT declare id="application.declaration"
data="http://www.aaa.co.jp/abc.sdf"
type="application/x-jam">
電話帳ビューア
</OBJECT>
  ~するソフトウェアです。ダウンロードするには
  <A ijam="#application.declaration">ここ</A>
  をクリック。
```

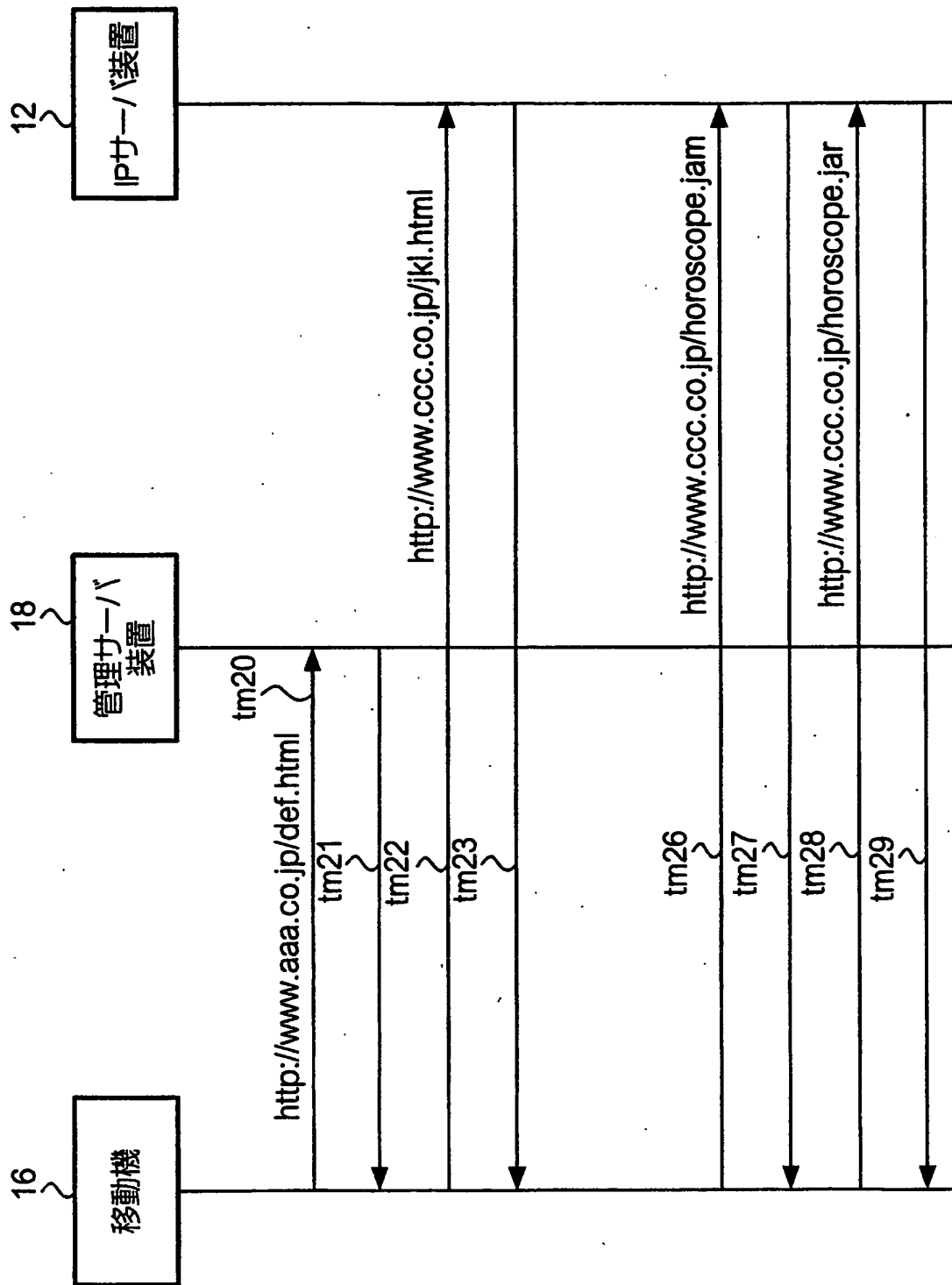
【図 1 5】



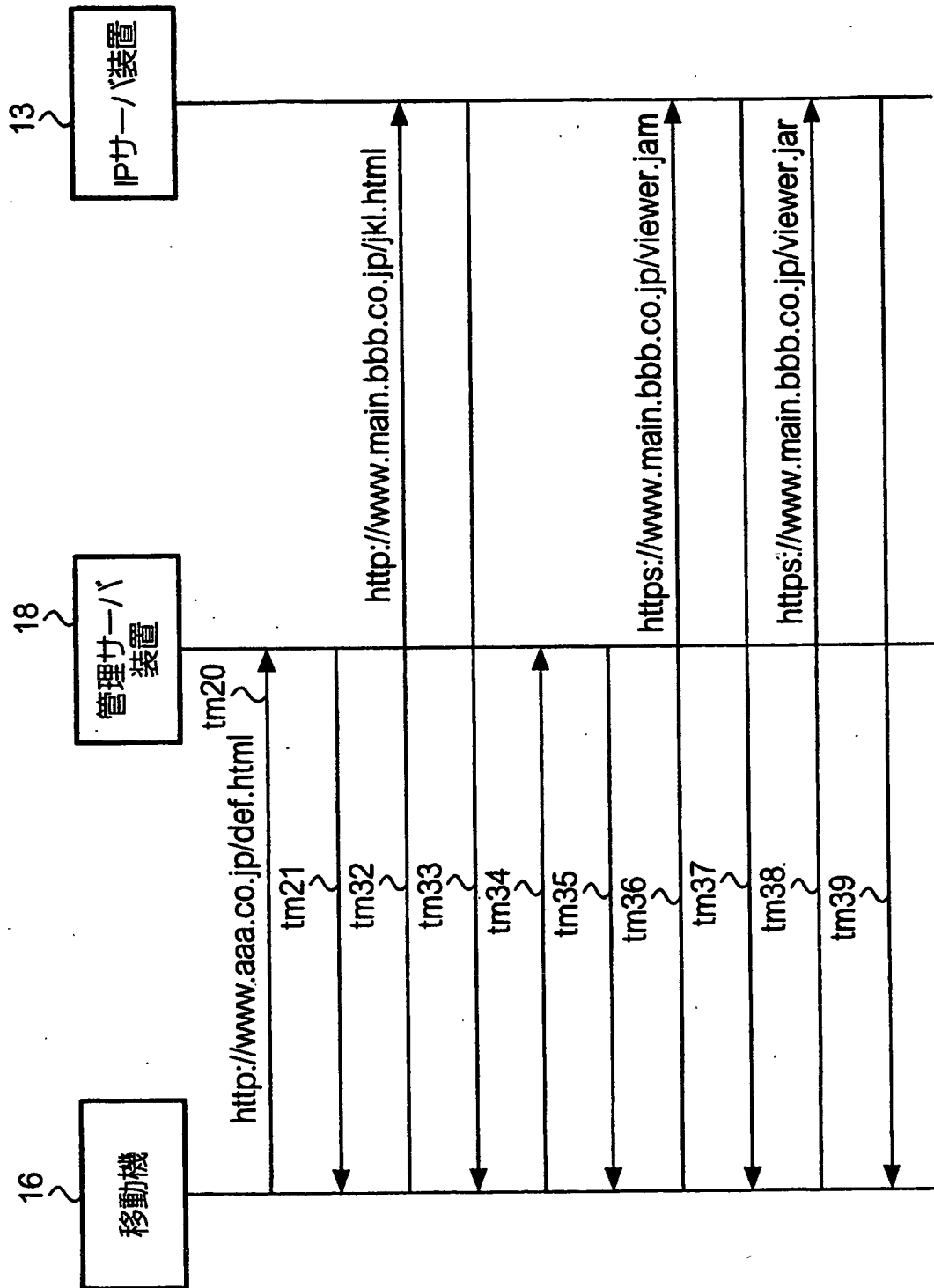
【図16】



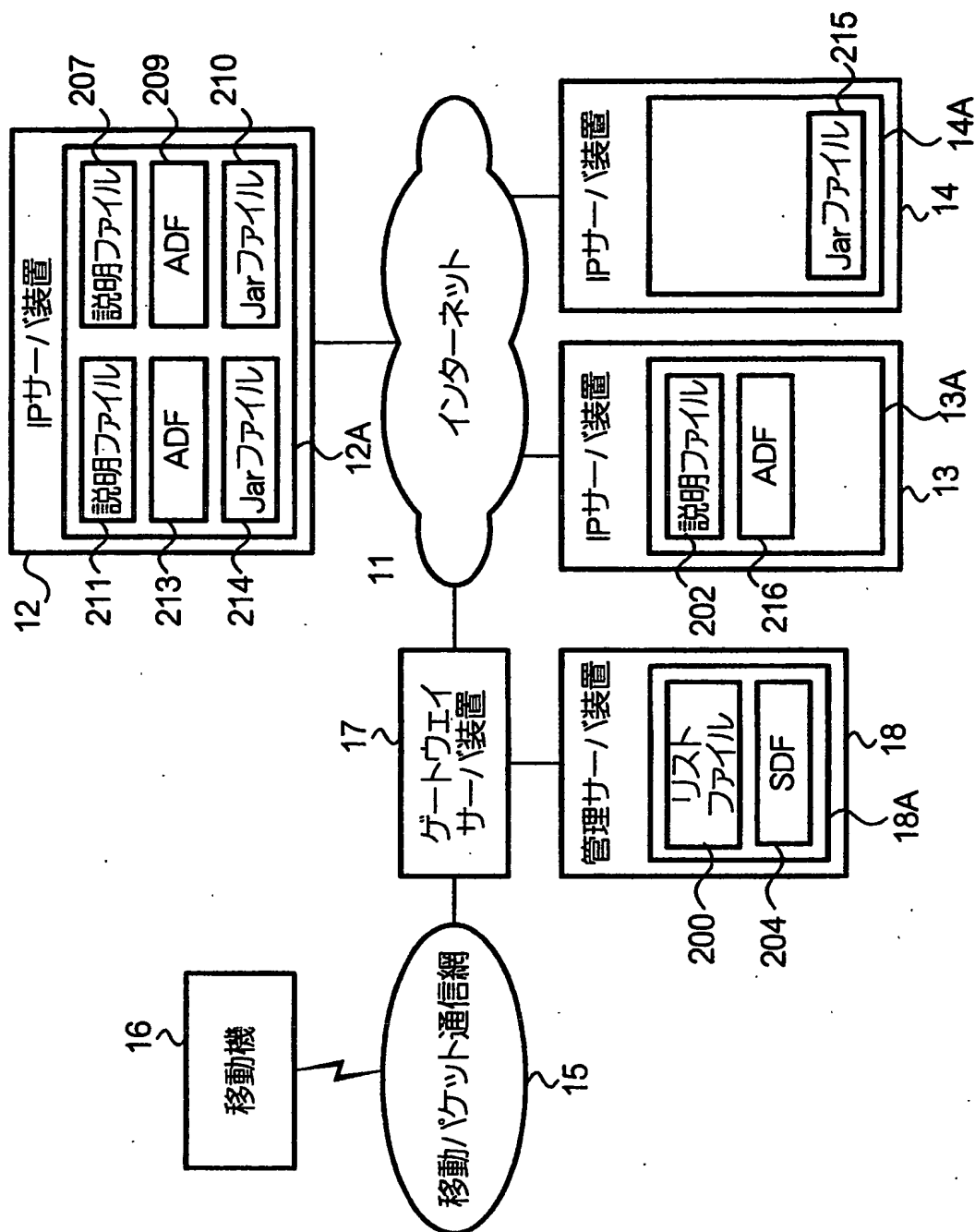
【図 1 7】



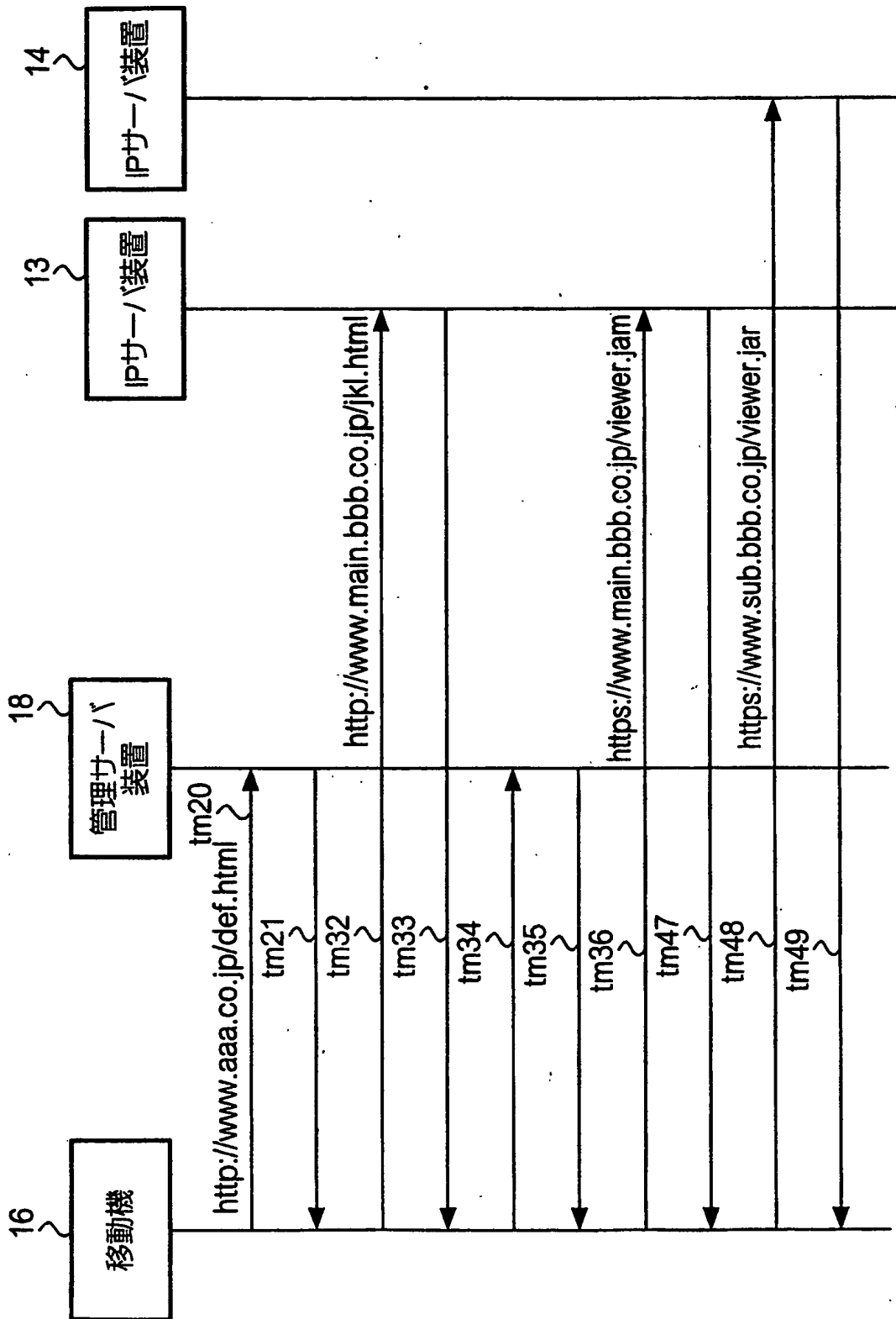
【図 18】



【図19】



【図 20】



【書類名】 要約書

【要約】

【課題】 IPの自由度を制限することなく、信頼性の保証されたJava-APP（Javaアプリケーション）ソフトウェアを移動機へ配信する。

【解決手段】 Java-APPソフトウェアを起動することができる移動機16が、信頼できる機関（移動パケット通信網15を管理する通信事業者）が管理する管理サーバ装置18からSDF（セキュリティ記述ファイル）204を受信し、このSDFに内包されているURLを用いてIPサーバ装置13からADF205を取得し、このADF205を用いてIPサーバ装置13からJarファイル206を取得し、これらのファイルを内包するJava-APPソフトウェアを自身にインストールする。このJava-APPソフトウェアを起動することで実現されるJava-APPは、SDF204に内包されているポリシー情報で表される権限の範囲内で動作する。

【選択図】 図8

出 願 人 履 歴 情 報

識別番号 [392026693]

1. 変更年月日	2000年 5月19日
[変更理由]	名称変更
住 所	東京都千代田区永田町二丁目11番1号
氏 名	株式会社エヌ・ティ・ティ・ドコモ